

# **ORAN SIM CE 5.2 ATI Security RN**

ORAN SIM CE 5.2 - Content

*16-January-2026*

## **Notices Copyright Notice ©**

Keysight Technologies 2005 - 2026

No part of this document may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Keysight Technologies, Inc. as governed by United States and international copyright laws.

## **Warranty**

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Keysight disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Keysight shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Keysight and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

## **Technology Licenses**

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

## **U.S. Government Rights**

The Software is "commercial computer software," as defined by Federal Acquisition Regulation ("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at <http://www.keysight.com/find/sweula> or <https://support.ixiacom.com/supportservices/warranty-license-agreements>. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Key-sight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data. 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

# Release Overview

## Table of Contents

### 1. [What is New](#)

- [641 New Exploits](#)
- [388 New Malware Samples](#)

### 2. [Full Content List](#)

- [3107 Exploits](#)
- [6755 Malware Samples](#)

For a complete listing of all the new features included in this release, please refer to the '[What is New](#)' section. For a complete listing of all the existing content included in this release, please refer to the '[Full Content List](#)' section.

# What is New

## New Exploits (641)

Attack profile that aims to simulate misuse of a particular vulnerability.

Name	References	Description
Strike Apache Struts REST Plugin OGNL Expression Code Execution Vulnerability	CVE: 2016-3087	This strike exploits a code execution vulnerability in Apache Struts. The vulnerability resides in the handleDynamicMethodInvocation() method of the RestActionMapper class when processing OGNL expressions with Direct Method Invocation enabled. A remote attacker can leverage this flaw by sending a crafted HTTP request, allowing arbitrary code execution with the privileges of the server.
Strike Moxa SoftCMS getcaminfo.asp VWID Parameter SQL Injection Vulnerability	CVE: 2016-5792	This strike exploits a SQL injection vulnerability in Moxa SoftCMS. The vulnerability exists due to improper sanitization of user-supplied input in the VWID parameter of the getcaminfo.asp page. A remote attacker could leverage this flaw by sending a specially crafted HTTP request, potentially leading to unauthorized database access, information disclosure, and remote code execution.
Strike Oracle Identity Manager Default Credentials Vulnerability	CVE: 2017-10151	This strike exploits an authentication weakness vulnerability in Oracle Identity Manager. The vulnerability exists due to the presence of default credentials in the WebLogic Server Administration Console and Enterprise Manager interfaces. A remote attacker can leverage this flaw to gain administrator-level privileges on the target system.
Strike HPE Intelligent Management Center FileDownloadServlet Directory Traversal Vulnerability	CVE: 2017-5795	This strike exploits a directory traversal vulnerability in HPE Intelligent Management Center. The vulnerability resides in the FileDownloadServlet due to improper sanitization of the fileName parameter in HTTP GET requests. A remote attacker can leverage this flaw to access and disclose arbitrary file contents from the server.
Strike Advantech WebAccess WADashboard Arbitrary File Overwrite Vulnerability	CVE: 2018-15705	This strike exploits an arbitrary file overwrite vulnerability in Advantech WebAccess SCADA WADashboard. The vulnerability exists due to improper validation of the folderpath parameter in HTTP requests, allowing directory traversal sequences to bypass restrictions. A remote, authenticated attacker can leverage this flaw to write arbitrary files to the server's file system, potentially leading to remote code execution.
Strike Zoho ManageEngine OpManager SQL Injection in Alarms API	CVE: 2018-20338	This strike exploits a SQL injection vulnerability in Zoho ManageEngine OpManager. The vulnerability resides in the insufficient validation of the "filters" parameter in HTTP requests to the listAlarms API. A remote, authenticated attacker could leverage this flaw by sending crafted HTTP requests containing malicious SQL queries, leading to arbitrary SQL code execution on the application's database.

Name	References	Description
Strike Schneider Electric IIoT Monitor Server downloadCSV.jsp Directory Traversal Vulnerability	CVE: 2018-7835	This strike exploits a directory traversal vulnerability in Schneider Electric IIoT Monitor Server. The vulnerability exists due to improper validation of the file parameter in requests to the downloadCSV.jsp endpoint. A remote, unauthenticated attacker could leverage this flaw to access and disclose the contents of arbitrary files accessible by the SYSTEM user.
Strike Zoho ManageEngine Applications Manager SQL Injection in Popup_SLA.jsp (sid Parameter)	CVE: 2019-11448	This strike exploits a SQL injection vulnerability in Zoho ManageEngine Applications Manager. The vulnerability resides in the improper validation of the "sid" parameter in the Popup_SLA.jsp Java class. A remote, unauthenticated attacker could leverage this flaw to execute arbitrary SQL commands, potentially leading to database manipulation and remote code execution in the context of the application.
Strike HPE Intelligent Management Center Expression Language Injection Vulnerability cve_2019_11943	CVE: 2019-11943	This strike exploits an Expression Language injection vulnerability in HPE Intelligent Management Center. The vulnerability resides in the improper validation of the beanName parameter within the SoapConfigBean class. Exploiting this flaw allows a remote, authenticated attacker to execute arbitrary code on the target system with SYSTEM-level privileges.
Strike Squid Proxy Digest Authentication Nonce Pointer Disclosure Vulnerability	CVE: 2019-18679	This strike exploits an information disclosure vulnerability in Squid Proxy. The vulnerability resides in the improper construction of the nonce value used in HTTP Digest authentication. A remote attacker could exploit this vulnerability to obtain leaked pointer addresses, potentially bypassing ASLR and facilitating further attacks.
Strike CoDeSys V3 CmpWebServer Heap Buffer Overflow Vulnerability	CVE: 2019-18858	This strike exploits a heap-based buffer overflow vulnerability in the CoDeSys V3 runtime system's web server. The vulnerability arises from improper validation of user-supplied data in the HTTP header "3S-Repl-Content" when processing requests to the /WebVisuV3 endpoint. A remote, unauthenticated attacker can exploit this flaw by sending specially crafted HTTP requests, potentially leading to arbitrary code execution in the context of the server process.
Strike rConfig devices.inc.php SQL Injection Vulnerability	CVE: 2019-19207	This strike exploits an SQL injection vulnerability in the rConfig Network Device Configuration Tool. The vulnerability exists due to improper sanitization of the searchColumn and searchField parameters in the devices.inc.php script. A remote, authenticated attacker can leverage this flaw by sending specially crafted HTTP requests, potentially leading to the execution of arbitrary SQL commands on the database of the target server.
Strike HPE Intelligent Management Center Expression Language Injection Vulnerability	CVE: 2019-5370	This strike exploits an Expression Language injection vulnerability in HPE Intelligent Management Center. The vulnerability resides in the IctTableExportToCSVBean class, specifically in the handling of the beanName HTTP request parameter. A remote attacker, after bypassing authentication or using valid credentials, can exploit this flaw by sending a crafted request, leading to arbitrary code execution with SYSTEM-level privileges.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike rConfig compliancepolicies.inc.php Unauthenticated SQL Injection Vulnerability	CVE: 2020-10546	This strike exploits a SQL injection vulnerability in the rConfig Network Device Configuration Tool. The vulnerability exists due to insufficient input validation in the compliancepolicies.inc.php script when processing HTTP request parameters. A remote, unauthenticated attacker can leverage this flaw to execute arbitrary SQL commands on the database, potentially leading to unauthorized data manipulation or access.
Strike OpenEMR phpGACL edit_group.php SQL Injection Vulnerability	CVE: 2020-13568	This strike exploits a SQL injection vulnerability in the OpenEMR phpGACL edit_group.php script. The vulnerability arises from improper validation of user-supplied input in the "parent_id" parameter during HTTP POST requests. A remote authenticated attacker can leverage this flaw to execute arbitrary SQL commands, potentially leading to the disclosure of sensitive information and further system compromise.
Strike Zoho ManageEngine OpManager Directory Traversal Vulnerability cve_2020_13818	CVE: 2020-13818	This strike exploits a directory traversal vulnerability in Zoho ManageEngine OpManager. The vulnerability resides in the improper validation of URI paths within the OpmSkipFilter::doFilter() method. A remote, unauthenticated attacker could leverage this flaw by sending specially crafted requests, potentially leading to arbitrary file read and disclosure of sensitive information on the target server.
Strike Cacti color.php SQL Injection Vulnerability	CVE: 2020-14295	This strike exploits a SQL injection vulnerability in Cacti. The vulnerability exists due to improper sanitization of the "filter" parameter in the color.php script. A remote, authenticated attacker could leverage this flaw to execute arbitrary SQL commands on the database, potentially leading to remote code execution on the target server.
Strike Zoho ManageEngine Applications Manager SQL Injection in AlertRes_Mtrgrp.jsp	CVE: 2020-15533	This strike exploits a SQL injection vulnerability in Zoho ManageEngine Applications Manager. The vulnerability exists due to insufficient validation of the "sid" parameter in the AlertRes_Mtrgrp.jsp servlet. A remote, unauthenticated attacker could leverage this flaw to execute arbitrary SQL commands, potentially leading to database manipulation and arbitrary code execution with SYSTEM privileges.
Strike Oracle Business Intelligence AMF Insecure Deserialization Vulnerability	CVE: 2020-2950	This strike exploits an insecure deserialization vulnerability in Oracle Business Intelligence. The vulnerability is located in the handling of AMF3 objects marked as externalizable within the BiRemotingServlet component. Exploiting this vulnerability allows a remote, unauthenticated attacker to execute arbitrary code in the security context of the affected server.
Strike Zoho ManageEngine Applications Manager SQL Injection Vulnerability in UriCollector Class	CVE: 2020-35765	This strike exploits a SQL injection vulnerability in Zoho ManageEngine Applications Manager. The vulnerability resides in the improper validation of the `resourceid` parameter within the `doFilter()` method of the `UriCollector` Java class. A remote, authenticated attacker could leverage this flaw by sending a crafted HTTP request, leading to the execution of arbitrary SQL statements and potentially arbitrary code in the context of the SYSTEM user.

Name	References	Description
Strike Rockwell Automation FactoryTalk RNADiagnosticsSrv Insecure Deserialization	CVE: 2020-6967	This strike exploits an insecure deserialization vulnerability in Rockwell Automation FactoryTalk Diagnostics. The vulnerability resides in the RNADiagnosticsSrv.exe component, specifically in the OnStart() method, which improperly handles serialized data. A remote, unauthenticated attacker could exploit this vulnerability by sending a maliciously crafted serialized object, leading to arbitrary code execution under the SYSTEM security context.
Strike Jenkins Generic Webhook Trigger Plugin XXE Vulnerability	CVE: 2021-21669	This strike exploits an XML External Entity (XXE) vulnerability in the Jenkins Generic Webhook Trigger Plugin. The vulnerability resides in the resolveXPath function, which improperly handles XML data in HTTP POST requests. A remote authenticated attacker with specific permissions could exploit this flaw to access and disclose the contents of arbitrary files readable by the Jenkins server.
Strike Advantech R-SeeNet ping.php Command Injection Vulnerability	CVE: 2021-21805	This strike exploits a command injection vulnerability in Advantech R-SeeNet. The vulnerability exists due to insufficient validation of the "hostname" parameter in the ping.php script. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted HTTP request, leading to arbitrary command execution with the privileges of the web server on the target system.
Strike Oracle E-Business Suite Sales Offline Infinite Loop Denial of Service Vulnerability	CVE: 2021-2190	This strike exploits an infinite loop vulnerability in the Sales Offline component of Oracle E-Business Suite. The vulnerability is located in the improper handling of HTTP POST requests with a Content-Length header value of 0 in the aslAuthincps.jsp file. Exploiting this vulnerability allows a remote, unauthenticated attacker to cause excessive CPU usage, potentially leading to denial of service conditions on the target server.
Strike Oracle E-Business Suite Knowledge Management Stored Cross-Site Scripting Vulnerability	CVE: 2021-2198	This strike exploits a stored cross-site scripting vulnerability in Oracle E-Business Suite Knowledge Management. The vulnerability resides in the improper sanitization of user-supplied input when handling time period definitions in JSP files. An authenticated attacker with administrative privileges could exploit this flaw to execute arbitrary script code in the browsers of users visiting the affected page.
Strike Advantech iView SQL Injection Vulnerability in ZTPConfigTable	CVE: 2021-22654	This strike exploits a SQL injection vulnerability in Advantech iView. The vulnerability exists due to insufficient validation of user-supplied input in the ZTPConfigTable Java class when processing HTTP request parameters. A remote, unauthenticated attacker could leverage this flaw by sending specially crafted requests, potentially leading to the execution of arbitrary SQL commands, unauthorized data access, or further system compromise.
Strike Eaton IPM Arbitrary File Deletion via Directory Traversal	CVE: 2021-23278	This strike exploits an arbitrary file deletion vulnerability in Eaton Intelligent Power Manager. The vulnerability exists due to insufficient input validation in the handling of HTTP parameters in the maps_srv.js and node_upgrade_srv.js scripts. A remote, authenticated attacker could leverage this flaw to delete arbitrary files on the target system, potentially leading to system compromise.

Name	References	Description
Strike Eaton Intelligent Power Management Arbitrary File Deletion via Directory Traversal	CVE: 2021-23279	This strike exploits an arbitrary file deletion vulnerability in Eaton Intelligent Power Management. The vulnerability resides in the meta_driver_srv.js script due to insufficient input validation of HTTP request parameters. A remote, unauthenticated attacker can exploit this flaw to delete arbitrary files on the target system, potentially leading to system compromise.
Strike Oracle BI Publisher JNDI Injection Vulnerability in SchedulerConfigPage11g	CVE: 2021-2391	This strike exploits a JNDI injection vulnerability in Oracle Business Intelligence Publisher. The vulnerability exists due to insufficient validation of the DB.CFG.JNDIName HTTP request parameter in the SchedulerConfigPage11g class. A remote, authenticated attacker can leverage this flaw by sending a specially crafted request, leading to the execution of arbitrary code on the server through the retrieval of a malicious serialized object.
Strike Oracle Business Intelligence Arbitrary File Upload Vulnerability	CVE: 2021-2392	This strike exploits an arbitrary file upload vulnerability in Oracle Business Intelligence. The vulnerability exists due to insufficient validation of the filename parameter in the UploadFndDBCPPage class. A remote, authenticated attacker could leverage this flaw to upload malicious files, potentially leading to privilege escalation or denial of service.
Strike Oracle BI Publisher JNDI Injection Vulnerability in UpdateConnectionServlet	CVE: 2021-2396	This strike targets a JNDI injection vulnerability in Oracle Business Intelligence Publisher. The issue arises from improper sanitization of the JNDINameField parameter in HTTP requests to the UpdateConnectionServlet. A remote, authenticated attacker could exploit this flaw to trigger a JNDI lookup on an attacker-controlled server, potentially leading to the execution of arbitrary code on the affected system.
Strike Apache OFBiz Insecure Deserialization Vulnerability	CVE: 2021-26295	This strike exploits an insecure deserialization vulnerability in Apache OFBiz. The vulnerability arises from improper handling of serialized objects within SOAP requests. A remote, unauthenticated attacker can exploit this flaw by sending a crafted payload, leading to arbitrary code execution on the affected system.
Strike Zoho ManageEngine AD SelfService Plus Command Injection Vulnerability	CVE: 2021-28958	This strike exploits a command injection vulnerability in Zoho ManageEngine AD SelfService Plus. The vulnerability arises from improper sanitization of user-supplied input during password change requests. A remote attacker could leverage this flaw to execute arbitrary commands on the server with the privileges of the web application.
Strike Apache OFBiz Insecure Deserialization Vulnerability cve_2021_30128	CVE: 2021-30128	This strike exploits an insecure deserialization vulnerability in Apache OFBiz. The vulnerability arises from improper validation of serialized objects within the <cus-obj> XML element in SOAP requests. A remote, unauthenticated attacker could leverage this flaw by sending a crafted payload, leading to arbitrary code execution on the affected system.
Strike Apache Tapestry ContextAssetRequestHandler Information Disclosure Vulnerability	CVE: 2021-30638	This strike exploits an information disclosure vulnerability in Apache Tapestry. The vulnerability resides in the ContextAssetRequestHandler class due to insufficient validation of user input when processing asset requests. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted HTTP request, potentially leading to unauthorized access and retrieval of sensitive files within the WEB-INF directory.

Name	References	Description
Strike Microsoft Visual Studio Code Remote-Containers Extension Remote Code Execution Vulnerability	CVE: 2021-31213	This strike exploits a remote code execution vulnerability in the Remote - Containers Extension for Microsoft Visual Studio Code. The vulnerability resides in the design flaw of the "Clone Repository in Container Volume" feature, which fails to adequately warn users about the risks of cloning untrusted repositories. A remote attacker could exploit this vulnerability by tricking a user into cloning a malicious repository, leading to the execution of arbitrary code with root-level privileges.
Strike SolarWinds Network Performance Monitor Insecure Deserialization Vulnerability	CVE: 2021-31474	This strike exploits an insecure deserialization vulnerability in SolarWinds Network Performance Monitor. The vulnerability resides in the FromJson() method of the SolarWinds.Serialization.Json.SerializationHelper class within the OrionWeb.dll component. A remote, authenticated attacker can leverage this flaw by sending a crafted serialized object to the vulnerable endpoint, leading to arbitrary code execution under the NETWORK SERVICE user context.
Strike Flarum Core Reflected and Stored Cross-Site Scripting Vulnerability	CVE: 2021-32671	This strike exploits a cross-site scripting vulnerability in the Flarum Core application. The vulnerability resides in the translation library, specifically in the preprocessParameters() method of Translators, which fails to properly sanitize HTML markup. Exploiting this vulnerability allows a remote attacker to execute arbitrary script code in the security context of the browser of any user interacting with the affected pages.
Strike Advantech iView runProViewUpgrade Command Injection Vulnerability	CVE: 2021-32930	This strike exploits a command injection vulnerability in Advantech iView. The vulnerability exists due to insufficient input validation in the `fwfilename` parameter of the `runProViewUpgrade` method within the `NetworkServlet` class. A remote, unauthenticated attacker could leverage this flaw by sending a specially crafted HTTP request, leading to the execution of arbitrary commands with SYSTEM-level privileges.
Strike SolarWinds Orion Platform RenderControl.aspx Insecure Deserialization Vulnerability	CVE: 2021-35215	This strike exploits an insecure deserialization vulnerability in the SolarWinds Orion Platform. The vulnerability resides in the RenderControl.aspx endpoint, where user-supplied JSON data is insufficiently validated. A remote, authenticated attacker can leverage this flaw to execute arbitrary code on the target system with NETWORK SERVICE privileges.
Strike SolarWinds Orion Patch Manager Insecure Deserialization Vulnerability	CVE: 2021-35216	This strike exploits an insecure deserialization vulnerability in the SolarWinds Orion Patch Manager Web Console. The vulnerability resides in the handling of the ThwackData parameter within the EditTopXX.aspx endpoint. A remote, authenticated attacker could leverage this flaw by sending a crafted serialized object, leading to remote code execution under the NETWORK SERVICE security context.
Strike OpenSSL SM2 Decryption Buffer Overflow Vulnerability	CVE: 2021-3711	This strike exploits a buffer overflow vulnerability in the OpenSSL library. The vulnerability arises from an incorrect calculation of the plaintext size during SM2 decryption in the sm2_plaintext_size function. A remote attacker can exploit this flaw by sending specially crafted SM2 encrypted data, potentially leading to denial of service conditions.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Centreon csv_HostGroupLogs.php SQL Injection Vulnerability	CVE: 2021-37556	This strike exploits an SQL injection vulnerability in the Centreon Web Application. The vulnerability exists due to insufficient input validation of the "start" and "end" parameters in the csv_HostGroupLogs.php script. A remote, authenticated attacker could leverage this flaw to execute arbitrary SQL commands on the database, potentially leading to unauthorized data manipulation or further exploitation.
Strike Centreon generateImage.php SQL Injection Vulnerability	CVE: 2021-37557	This strike exploits an SQL injection vulnerability in the Centreon web application. The vulnerability is located in the generateImage.php script, specifically in the handling of the index parameter within HTTP requests. Exploiting this vulnerability allows a remote, authenticated attacker to execute arbitrary SQL commands on the database, potentially leading to unauthorized data manipulation or further compromise of the system.
Strike Zoho ManageEngine ADManager Plus Unrestricted File Upload Vulnerability	CVE: 2021-37918	This strike exploits an unrestricted file upload vulnerability in Zoho ManageEngine ADManager Plus. The vulnerability resides in the ModifyPhotoAction class, specifically in the cachePhotosBeforeImport() method, which fails to properly validate the file type of uploaded files. A remote authenticated attacker can leverage this flaw by uploading a malicious file, potentially leading to arbitrary code execution with SYSTEM-level privileges.
Strike Delta Industrial Automation DIAEnergie SQL Injection Vulnerability in HandlerAlarmGroup.aspx	CVE: 2021-38393	This strike exploits an SQL injection vulnerability in Delta Industrial Automation DIAEnergie. The vulnerability is located in the HandlerAlarmGroup.ashx endpoint due to insufficient input validation of the agid parameter. A remote, unauthenticated attacker could leverage this flaw to execute arbitrary SQL commands, potentially leading to code execution with NT SERVICE\MSSQLSERVER privileges.
Strike Zoho ManageEngine OpManager SQL Injection in getDataCollectionFailureReason Method	CVE: 2021-40493	This strike exploits a SQL injection vulnerability in Zoho ManageEngine OpManager. The vulnerability resides in the getDataCollectionFailureReason method, which fails to properly validate HTTP request parameters such as pollingObject and deviceName. A remote, authenticated attacker could leverage this flaw by sending crafted HTTP requests, leading to the execution of arbitrary SQL commands on the application's database.
Strike Zoho ManageEngine Network Configuration Manager SQL Injection Vulnerability	CVE: 2021-41081	This strike exploits a SQL injection vulnerability in Zoho ManageEngine Network Configuration Manager. The vulnerability is located in the CONFIG_SEARCH_CRITERIA parameter of the configuration search operation, where input is improperly validated. Exploiting this vulnerability allows a remote, authenticated attacker to execute arbitrary SQL commands, potentially compromising the underlying database.
Strike Delta Industrial Automation DIAEnergie Stored Cross-Site Scripting Vulnerability cve_2021_44544	CVE: 2021-44544	This strike exploits a stored cross-site scripting vulnerability in Delta Industrial Automation DIAEnergie. The vulnerability exists due to insufficient input validation in the HandlerEnergyType.ashx endpoint when processing the "name," "kid," and "descr" parameters. A remote attacker can exploit this flaw to execute arbitrary JavaScript code in the context of the victim's browser, potentially leading to unauthorized actions or data exposure.

Name	References	Description
Strike Tiny File Manager Directory Traversal and Arbitrary File Write Vulnerability	CVE: 2021-45010	This strike exploits a directory traversal vulnerability in Tiny File Manager. The vulnerability arises from insufficient validation of the "fullpath" parameter during file upload operations. A remote, authenticated attacker can leverage this flaw to perform directory traversal and arbitrary file write, potentially leading to remote code execution under the web server's security context.
Strike Apache Kylin dumpProjectDiagnosisInfo Command Injection Vulnerability	CVE: 2021-45456	This strike exploits a command injection vulnerability in Apache Kylin. The vulnerability resides in the dumpProjectDiagnosisInfo method due to improper validation of user-supplied project names. A remote authenticated attacker could leverage this flaw by crafting a malicious project name and sending it to the vulnerable REST API endpoint, leading to arbitrary command execution in the context of the server process.
Strike WordPress TI WooCommerce Wishlist Plugin item_id Blind SQL Injection Vulnerability	CVE: 2022-0412	This strike exploits a blind SQL injection vulnerability in the TI WooCommerce Wishlist Plugin for WordPress. The vulnerability exists due to improper sanitization of the user-supplied `item_id` parameter in the `get_wishlist_by_product_id()` function. Exploiting this vulnerability allows a remote, unauthenticated attacker to retrieve arbitrary information from the target database.
Strike Dolibarr ERP-CRM Menu Editor Code Injection Vulnerability	CVE: 2022-0819	This strike exploits a code injection vulnerability in the Dolibarr ERP/CRM software. The vulnerability exists due to insufficient input validation in the "Menu editor" module, specifically in the handling of the "perms" and "enabled" parameters. Exploiting this vulnerability allows a remote, authenticated attacker to execute arbitrary PHP code, potentially leading to remote code execution on the target server.
Strike WordPress Photo Gallery Plugin SQL Injection via filter_tag Parameter	CVE: 2022-1281	This strike targets a SQL injection vulnerability in the Photo Gallery plugin for WordPress. The issue arises from improper sanitization of the "filter_tag" parameter in HTTP requests. Exploiting this flaw allows a remote, unauthenticated attacker to execute arbitrary SQL commands, potentially leading to unauthorized access to sensitive database information.
Strike Pimcore GridHelperService SQL Injection Vulnerability	CVE: 2022-1429	This strike exploits a SQL injection vulnerability in Pimcore. The vulnerability exists due to improper input validation in the /grid-proxy, /get-export-jobs, and /get-batch-jobs APIs. A remote, authenticated attacker could leverage this flaw by sending specially crafted requests, potentially leading to unauthorized database access and manipulation.
Strike WordPress Events Made Easy Plugin lang Parameter SQL Injection Vulnerability	CVE: 2022-1905	This strike exploits a SQL injection vulnerability in the Events Made Easy plugin for WordPress. The vulnerability exists due to insufficient sanitization of the "lang" parameter in HTTP requests. A remote, unauthenticated attacker could leverage this flaw to execute arbitrary SQL commands, potentially leading to unauthorized access to sensitive data in the database.

Name	References	Description
Strike Lansweeper AssetActions SQL Injection Vulnerability	CVE: 2022-21210	This strike exploits an SQL injection vulnerability in Lansweeper. The vulnerability exists due to improper sanitization of user-supplied input in the "Mass Edit Assets" functionality. A remote, authenticated attacker can leverage this flaw to execute arbitrary SQL commands, potentially gaining unauthorized access to or manipulating the underlying database.
Strike Lansweeper GetAssetsByGroupId SQL Injection Vulnerability	CVE: 2022-21234	This strike exploits an SQL injection vulnerability in Lansweeper. The vulnerability exists due to improper sanitization of user-supplied input in the "order" parameter of the GetAssetsByGroupId function. A remote, authenticated attacker could leverage this flaw by sending a crafted HTTP request, potentially leading to remote code execution under the security context of the database service.
Strike Advantech iView SQL Injection in findTaskMgrItems Parameters	CVE: 2022-2135	This strike targets a SQL injection vulnerability in Advantech iView. The issue arises from insufficient input validation for the "sort_field" and "sort_type" parameters in the "findTaskMgrItems" process. Exploiting this flaw allows a remote, unauthenticated attacker to execute arbitrary SQL commands on the affected server.
Strike Advantech iView SQL Injection in set_useraccount UserName Parameter	CVE: 2022-2136	This strike targets a SQL injection vulnerability in Advantech iView. The issue arises from insufficient input validation of the UserName parameter in the set_useraccount process. Exploiting this flaw allows a remote, authenticated attacker to execute arbitrary SQL commands, potentially leading to remote code execution with SYSTEM-level privileges.
Strike Lansweeper HelpdeskSetupActions SQL Injection Vulnerability	CVE: 2022-22149	This strike exploits an SQL injection vulnerability in Lansweeper. The vulnerability exists due to improper sanitization of user-supplied input in the EditSetting() method of the HelpdeskSetupActions component. A remote, authenticated attacker can leverage this flaw to execute arbitrary SQL commands, potentially leading to remote code execution under the database service.
Strike H2 Database Console Remote Code Execution via Malformed JDBC URL	CVE: 2022-23221	This strike exploits a remote code execution vulnerability in the H2 Database Console. The vulnerability arises from improper input validation when processing specific JDBC URLs. A remote, unauthenticated attacker can exploit this flaw by sending a crafted request, potentially leading to arbitrary code execution with the privileges of the H2 process.
Strike Parse Server DatabaseController Prototype Pollution Vulnerability	CVE: 2022-24760	This strike exploits a prototype pollution vulnerability in Parse Server. The vulnerability exists due to improper input validation in the DatabaseController when handling JSON data in HTTP POST and PUT requests. A remote, unauthenticated attacker could exploit this vulnerability to inject or modify properties in Object.prototype, potentially leading to denial of service or remote code execution.
Strike WordPress WP Statistics Plugin Stored Cross-Site Scripting Vulnerability	CVE: 2022-25305	This strike exploits a stored cross-site scripting vulnerability in the WordPress WP Statistics plugin. The vulnerability exists due to insufficient input validation of the "ip," "browser," and "platform" parameters in the class-wp-statistics-visitor.php file. Exploiting this vulnerability allows a remote, unauthenticated attacker to execute arbitrary JavaScript code in the context of a user's browser.

Name	References	Description
Strike Studio-42 elFinder Directory Traversal Vulnerability	CVE: 2022-26960	This strike exploits a directory traversal vulnerability in Studio-42 elFinder. The vulnerability exists due to insufficient validation of user-supplied paths in the target and targets parameters. A remote, unauthenticated attacker can leverage this flaw to access files outside the intended web root, potentially leading to arbitrary code execution under the web server's security context.
Strike WWBN AVideo Command Injection via downloadURL Parameter	CVE: 2022-32572	This strike exploits a command injection vulnerability in WWBN AVideo. The vulnerability exists due to insufficient sanitization of the `downloadURL` parameter in HTTP requests. A remote, authenticated attacker could leverage this flaw to execute arbitrary commands on the server, potentially leading to remote code execution.
Strike Advantech iView ConfigurationServlet SQL Injection Vulnerability	CVE: 2022-3323	This strike exploits a SQL injection vulnerability in Advantech iView. The vulnerability is located in the ConfigurationServlet, specifically in the improper validation of the column_value parameter. Exploiting this vulnerability allows a remote, unauthenticated attacker to execute crafted SQL queries, potentially leading to information disclosure.
Strike Trend Micro Mobile Security web_service.dll Path Traversal Vulnerability	CVE: 2023-32521	This strike exploits a path traversal vulnerability in Trend Micro Mobile Security. The vulnerability exists due to improper validation of user-supplied file paths in the web_service.dll component. A remote, unauthenticated attacker could leverage this flaw to delete arbitrary files on the system under the security context of the IIS Anonymous Authentication account.
Strike Splunk Enterprise Arbitrary File Write via XSLT Stylesheets	CVE: 2023-46214	This strike targets an arbitrary file write vulnerability in Splunk Enterprise. The issue resides in the insufficient validation of XSLT stylesheets within the getJobAsset method of the search.py script. Exploiting this vulnerability allows a remote, authenticated attacker to create or overwrite arbitrary files, potentially leading to arbitrary code execution under the context of the Splunk process.
Strike WordPress Royal Elementor Addons Plugin Unrestricted File Upload Vulnerability	CVE: 2023-5360	This strike exploits an unrestricted file upload vulnerability in the WordPress Royal Elementor Addons and Templates plugin. The vulnerability arises from insufficient validation of user-supplied input during file upload processing. A remote attacker can leverage this flaw to upload malicious files, potentially leading to remote code execution within the context of the PHP interpreter.
Strike WordPress Ultimate Member Plugin SQL Injection via Sorting Parameter	CVE: 2024-1071	This strike exploits a time-based blind SQL injection vulnerability in the WordPress Ultimate Member plugin. The vulnerability exists due to improper input validation of the "sorting" parameter in the ajax_get_members() function. A remote, unauthenticated attacker can leverage this flaw to execute arbitrary SQL commands, potentially leading to unauthorized access to sensitive database information.
Strike ConnectWise ScreenConnect InstallExtension Directory Traversal Vulnerability	CVE: 2024-1708	This strike exploits a directory traversal vulnerability in ConnectWise ScreenConnect. The vulnerability exists due to improper validation of file paths within ZIP archives during the extension installation process. A remote attacker could leverage this flaw to execute arbitrary code on the target server by crafting malicious ZIP files.

Name	References	Description
Strike Centreon Web Virtual Metrics SQL Injection Vulnerability	CVE: 2024-55573	This strike exploits an SQL injection vulnerability in Centreon Web. The vulnerability resides in the manageVMetric method of the centreonGraph.class.php script, specifically in the handling of the rpn_function parameter. A remote, authenticated attacker could leverage this flaw by sending specially crafted requests, leading to arbitrary SQL command execution on the target database.
Strike Centreon Web updateServiceHost SQL Injection Vulnerability	CVE: 2024-5723	This strike exploits an SQL injection vulnerability in Centreon Web. The vulnerability exists due to insufficient input validation in the updateServiceHost function within the DB-Func.php script. A remote, authenticated attacker could leverage this flaw by sending specially crafted requests, leading to the execution of arbitrary SQL commands on the target database.
Strike Reprise License Manager HTTP licfile Buffer Overflow		This strike exploits a buffer overflow vulnerability in Reprise License Manager. The vulnerability is due to improper validation of HTTP request licfile parameter. By exploiting this vulnerability an attacker could execute arbitrary scripts on the target machine.
Strike Domino Web Server Database Access - agentrunner.nsf		This strike attempts to access the /agentrunner.nsf database on a misconfigured Lotus Domino web server.
Strike Apache File Access .htgroup		This strike attempts to access an Apache configuration file over HTTP.
Strike Apache File Access .htpasswd		This strike attempts to access an Apache configuration file over HTTP.
Strike Apache File Access httpd.conf		This strike attempts to access an Apache configuration file over HTTP.
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 1	BID: 4294 CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 2	BID: 4294 CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 11	BID: 4294 CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 12	BID: 4294  CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.
Strike Apache Stronghold Server Information Disclosure		This strike attempts to access the Apache Stronghold stronghold-info page.
Strike Apache Stronghold Server Status Disclosure		This strike attempts to access the Apache Stronghold stronghold-status page.
Strike Sensitive File Access .svn-entries		This strike attempts to access a Subversion entries file in the web root.
Strike Apache System User Directory Access bin		This strike attempts to access a system user's web directory over HTTP.
Strike Apache System User Directory Access cron		This strike attempts to access a system user's web directory over HTTP.
Strike Apache System User Directory Access root		This strike attempts to access a system user's web directory over HTTP.
Strike Sensitive File Access ws_ftp.log		This strike attempts to access a WS_FTP transfer log file.
Strike Sensitive File Access WS_FTP.LOG		This strike attempts to access a WS_FTP transfer log file.
Strike Apache File Access .www_acl		This strike attempts to access an Apache configuration file over HTTP.
Strike Apache File Access .wwwacl		This strike attempts to access an Apache configuration file over HTTP.
Strike Apache File Access .wwwgroup		This strike attempts to access an Apache configuration file over HTTP.
Strike Apache File Access .wwwpasswd		This strike attempts to access an Apache configuration file over HTTP.
Strike Actionpoll index.php include Parameter PHP File Include	CVE: 2001-1296  BID: 3383	This strike exploits a PHP include flaw in the Actionpoll PHP voting application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Actionpoll index.php include_dir Parameter PHP File Include	CVE: 2001-1296  BID: 3383	This strike exploits a PHP include flaw in the Actionpoll PHP voting application.
Strike ActivePerl perlIS.dll Filename Overflow Variant 1	CVE: 2001-0815  BID: 3526	This strike exploits a buffer overflow in perlIS.dll in ActivePerl for Microsoft IIS when parsing requests containing a long filename ending in '.pl'.
Strike AdMentor Admin Remote SQL Injection	CVE: 2007-0575  BID: 22281	This strike exploits a remote SQL injection vulnerability in the AdMentor admin page
Strike Adobe Acrobat getAnnots Remote Code Execution (HTTP)	BID: 34736  CWE: 399  CVE: 2009-1492	This strike exploits a code execution vulnerability in Adobe Acrobat Reader.
Strike Adobe Flash plugin Transparent Object Clickjacking Vulnerability	CWE: 264  CVE: 2013-2866	This strike exploits a vulnerability in the Adobe flash plugin for the Google Chrome Browser on Macintosh OSX. The Flash vulnerability exists in the latest version of Chrome and allows for the victim's webcam's audio/video to be hijacked when handling CSS opacity settings that make the window transparent. Normal use of this plugin would prompt the user to allow or deny use to the requesting ip, but in this case it executes without a prompt.
Strike AOL 9.5 ActiveX SoapURL Buffer Overflow		This strike exploits a buffer overflow in an AOL 9.5 ActiveX control when calling the SoapURL function.
Strike Apache APR_PSPrintf Memory Corruption Vulnerability	CVE: 2003-0245  BID: 7723	This strike exploits a buffer overflow flaw in the Apache HTTP server.
Strike Apache apr- util IPv6 URI Parsing Buffer Overflow 1	CVE: 2004-0786	This strike exploits a vulnerability in the way Apache 2.0.35 - 2.0.50 parses IPv6 URI addresses. An attacker can request a malformed literal address which causes a buffer overflow and could potentially lead to code execution.
Strike Apache apr- util IPv6 URI Parsing Buffer Overflow 2	CVE: 2004-0786	This strike exploits a vulnerability in the way Apache 2.0.35 - 2.0.50 parses IPv6 URI addresses. An attacker can request a malformed literal address which causes a buffer overflow and could potentially lead to code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Apache Chunked Encoding Overflow - Apache Nosejob	CVE: 2002-0392 BID: 5033	This strike exploits a buffer overflow flaw in the Apache HTTP server. This strike is based on the nosejob.c proof-of-concept exploit.
Strike Apache Chunked Encoding Overflow - Apache Nosejob (Evade)	CVE: 2002-0392 BID: 5033	This strike exploits a buffer overflow flaw in the Apache HTTP server. This strike is based on the nosejob.c proof-of-concept exploit.
Strike Apache Chunked Encoding Overflow - Apache Scalp	CVE: 2002-0392 BID: 5033	This strike exploits a buffer overflow flaw in the Apache HTTP server. This strike is based on the scalp.c proof-of-concept exploit.
Strike Apache Chunked Encoding Overflow - Apache Scalp (Evade)	CVE: 2002-0392 BID: 5033	This strike exploits a buffer overflow flaw in the Apache HTTP server. This strike is based on the scalp.c proof-of-concept exploit.
Strike Apache Struts2 code execution	CWE: 732  CVE: 2011-3923  BID: 51628	The strike exploits a malicious code execution vulnerability present in apache strust2. The attacker can execute command by sending crafted HTTP request.
Strike Apple Safari Javascript Multibyte Character Escaping DoS		This strike triggers a denial of service in the Apple Safari web browser when handling Javascript that escapes multibyte character strings.
Strike Apple Safari for Windows Beta feed --URL DoS Variant 1	BID: 24460	This strike exploits a denial of service flaw in Apple Safari for Windows Beta. This flaw is triggered when the browser attempts to open feed:// urls with special characters.
Strike AssetMan download_pdf.php pdf_file Parameter Directory Traversal	BID: 22921  CVE: 2007-1427	This strike exploits a directory traversal vulnerability in AssetMan
Strike Beautifier Core.php BEAUT_PATH Parameter PHP File Include	CVE: 2006-4044  BID: 19873	This strike exploits a PHP include flaw in the Beautifier web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer Frameset Null Pointer Dereference		This strike exploits a Denial of Service in Microsoft Internet Explorer. The vulnerability is triggered when a specific HTML element attribute is set to an unallowed value. By enticing a user to view a malicious web page, an attacker can cause the vulnerable browser to crash. NOTE: The vendor does not intend to issue a patch for this vulnerability.
Strike CA BrightStor ARCserve Backup r11.5 ActiveX AddColumn Buffer Overflow	CWE: 119 CVE: 2008-1472 BID: 28268	This strike exploits flaw in an ActiveX control that ships with CA Brightstor ARCserve Backup r11.5 that can be triggered by sending an overly long string as the first argument to the AddColumn method resulting in a buffer overflow and potentially leading to arbitrary code execution.
Strike Centreon Web Interface UserAlias Command Execution	EXPLOITDB : 40170	This strike exploits a vulnerability in Centreon Web Interface. The vulnerability is due to how Centreon utilizes the echo command for logging SQL errors. It is possible for an unauthenticated attacker to abuse this functionality to inject and execute commands remotely at the login screen.
Strike CHETCPASSWD System Shadow File Disclosure	CVE: 2002-2219 BID: 6472	This strike exploits a flaw in CHETCPASSWD that discloses the tail end of the system shadow file
Strike Clipbucket Arbitrary PHP Code Execution		This strike exploits a file upload vulnerability in Clipbucket web application. The vulnerability is due to improper validation of the user controlled input to the file uploading scripts. By exploiting this vulnerability, a remote, unauthenticated attacker can upload any file including PHP scripts and execute them on the target server. NOTE: When run in one-arm mode, target web application index needs to be available at http://[server].
Strike Clipbucket - Operating System Command Injection		This strike exploits a command injection vulnerability in Clipbucket web application. The vulnerability is due to improper input validation of the "file_name" parameter in HTTP requests to "file_uploader.php" script. By exploiting this vulnerability, a remote, unauthenticated attacker can execute arbitrary OS commands on the target server. NOTE: When run in one-arm mode, file_uploader.php script needs to be available at http://[server]/api/file_uploader.php. Test will create a file named "exploited" in the same location as the vulnerable script.
Strike CSLiveSupport csLiveSupport.cgi setup Parameter Code Execution	CVE: 2002-1751 BID: 4450	This strike exploits an arbitrary code execution flaw in the csLiveSupport website client support application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer mergeAttribues Property Handling Memory Corruption	CVE: 2007-0945 BID: 23769	Microsoft Internet Explorer contains a memory corruption vulnerability. The mergeAttribues method will copy the attributes, events, and styles from one DOM object to another without validating the type of object passed in. If attributes exist in the source object which do not exist in the destination object, those attributes may write in out-of-bounds memory, resulting in memory corruption. Successful exploitation may result in arbitrary code execution with user privileges or abnormal termination of Internet Explorer.
Strike Microsoft Internet Explorer cloneNode Dereferenced Pointer Memory Corruption	CWE: 399 CVE: 2007-3903 BID: 26816	Microsoft Internet Explorer contains a memory corruption vulnerability. If an element object is created with no variable referencing it, the memory will be freed during garbage collection. If cloneNode is then called on that object, which contains a pointer to the now freed memory, memory corruption could occur. Successful exploitation could lead to execution of arbitrary code or abnormal termination of Internet Explorer.
Strike Symantec appstream launchobj ActiveX code execution	CWE: 20 CVE: 2008-4388 BID: 33247	This strike exploits a Symantec appstream client launchobj ActiveX control code execution vulnerability which is due to no confirmation when executing the command in the ActiveX control. Remote attackers may do arbitrary file creation on the target system.
Strike HP Openview Network Node Manager ovalaunch HTTP Request Buffer Overflow	CWE: 119 CVE: 2008-4562 BID: 33668	This strike exploits a buffer overflow vulnerability in HP OpenView Network Node Manager (NMM). The vulnerability is due to insufficient validation of user-supplied data. By sending a specially crafted HTTP request an unauthenticated attacker could potentially execute arbitrary code on the target server.
Strike Free Download Manager torrent File String Buffer Overflow	CWE: 119 CVE: 2009-0184 BID: 33555 EXPLOITDB : 16634	This strike exploits a stack buffer overflow vulnerability in Free Download Manager. Multiple vulnerabilities can be triggered by use of overly long string values. By enticing a user to open a malicious file with the affected software, an attacker could execute arbitrary code.
Strike Oracle Secure Backup Administration Authentication Bypass < >	CVE: 2009-1977 BID: 35672	This strike exploits a authentication bypass inside Oracle's secure backup administration application. The vulnerability resides in the php script that handles authentication and is present due to an input validation error
Strike Oracle Secure Backup Administration Property Box Command Injection	CVE: 2009-1978 BID: 35678	This strike exploits a command injection vulnerability inside Oracle's Secure Backup Adminstration web interface. The vulnerability allows command injection by passing malicious URL encoded parameters to property_box.php script

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike HP OpenView NNM ovwebsnmpsrv Buffer Overflow	CWE: 119 CVE: 2009-4181 BID: 37343	This strike identifies a vulnerability in the ovwebsnmpsrv.exe service of HP OpenView's Network Node Manager. A buffer overflow exists when parsing the sel value of the request. The number of times this value is copied to a stack buffer of 400 bytes is determined by the OvwSelections parameter in the arg value.
Strike Novell eDirectory dhost stack buffer overflow	CWE: 119 CVE: 2009-4653 BID: 37009 BID: 36815	This strike exploits a Novell eDirectory dhost stack buffer overflow vulnerability which is due to bad input check the length of module name in HTTP request. Remote attackers may do arbitrary code execution on the target system.
Strike Novell eDirectory dhost httpstpk password buffer overflow	CWE: 119 CVE: 2009-4654 BID: 37042	This strike exploits a Novell eDirectory dhost httpstpk passwords buffer overflow vulnerability which is due to bad input check the length of sadminpwd and verifypwd. Remote attackers may do arbitrary code execution on the target system.
Strike Symantec IM Manager groupList Parameter SQL Injection	CWE: 89 CVE: 2010-0112 BID: 44299	This strike exploits a SQL injection vulnerability in the groupList parameter in the Symantec IM manager. This vulnerability is due to improper sanitization of an HTTP parameter. A remote attacker could exploit vulnerability to execute arbitrary SQL commands on the target system.
Strike Internet Explorer mergeAttributes Method Memory Corruption	CWE: 94 CVE: 2010-0247 BID: 37893	This strike exploits a vulnerability in Microsoft Internet Explorer. The mergeAttributes method is not properly validated, and when an object uses it with the object as the oSource parameter, the attributes are deleted. The object is then called, and because the attributes have been modified, memory corruption will occur.
Strike Viscom Software Movie Player Pro ActiveX Control Buffer Overflow	CWE: 119 CVE: 2010-0356	This strike exploits a buffer overflow in Viscom's Movie Player Pro ActiveX control MOVIEPLAYER.MoviePlayerCtrl.1. The strFontName parameter is not properly validated, and if an overly long string is received it will overflow the buffer.
Strike Novell Teaming File Upload Directory Traversal	CVE: 2010-2773 BID: 41795	This strike exploits a vulnerability in Novell's Teaming where a user may use a directory traversal exploit to clobber arbitrary files.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Sharepoint Malformed Request Code Execution Vulnerability	CVE: 2010-3964 BID: 45264	This strike exploits a code execution vulnerability in Microsoft Sharepoint Document Coversion Launcher service. The vulnerability is due to insufficient validation of SOAP requests sent to the service interface. By specially crafting a malicious SOAP request, an unauthenticated attacker could execute arbitrary commands on the server.
Strike Symantec IM Manager SQL Injection Vulnerability	CWE: 89 CVE: 2011-0553 BID: 49738	This strike exploits a SQL injection vulnerability in Symantec IM Manager. The vulnerability is due to a failure to properly validate parameters in HTTP requests to IMAdminLDAPConfig.asp. A remote attacker could exploit this vulnerability by enticing an authenticated user to view a malicious web page, resulting in execution of arbitrary SQL code against the IM Manager database.
Strike Cisco Unified Communications Manager Multiple SQL Injections	CWE: 89 CVE: 2011-1610	This strike exploits an SQL injection vulnerability in Cisco Unified Communications Manager. The vulnerability arises due to the lack of proper sanitation of user supplied arguments to xmldirectorylist.jsp, xmldirectorylist.utf-8.jsp, and xmldirectorylist.other.jsp. An unauthenticated remote attacker can access the vulnerable web service and inject an SQL query into a parameter, thus allowing an attacker to inject and execute arbitrary SQL commands, which can result in disclosure of sensitive information.
Strike Microsoft ASP .NET Forms Authentication Elevation of Privilege	CWE: 264 CVE: 2011-3416 BID: 51201	The Forms Authentication feature in the ASP.NET subsystem in Microsoft .NET Framework 1.1 SP1, 2.0 SP2, 3.5 SP1, 3.5.1, and 4.0 allows remote authenticated users to obtain access to arbitrary user accounts via a crafted username, aka "ASP.Net Forms Authentication Bypass Vulnerability."
Strike HP Managed printing Administration jobAcct Remote Command Execution	CWE: 22 CVE: 2011-4166 BID: 51174	This strike exploits a vulnerability in HP Managed Printing Administration web interface. A flaw in the MPAUploader.uploader.1 control, specifically in the UploadFiles functioncould allow a remote unauthenticated attacker to upload a file under the wwwroot directory. Version 2.6.3 and before are vulnerable.
Strike Microsoft Internet Explorer VML Use After Free CVE 2012-0155	CWE: 94 CVE: 2012-0155 BID: 51935	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when removing objects described in the Vector Markup Language (VML).
Strike IBM Tivoli Provisioning Manager SQL Injection	CWE: 89 CVE: 2012-0199	This strike exploits an SQL Injection in IBM Tivoli Provisioning Manager where an attacker can update underlying data. In particular, a user may upgrade their account to an administrator.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle GlassFish XSS	BID: 53136 CVE: 2012-0551	This strike exploits a cross site scripting flaw in the Oracle GlassFish. The remote attacker could use this vulnerability to do code execution attack in the target system.
Strike HP SiteScope Multiple Directory Traversal Vulnerabilities	CVE: 2012-3264 BID: 55273	This strike exploits a directory traversal vulnerability in HP SiteScope. The vulnerability is due to insufficient validation of user-supplied input by Upload/Download manager servlets while processing http requests. A remote attacker could exploit the vulnerability to download, or upload and execute, arbitrary files to/from the target server via relative or full directory paths.
Strike Avaya's IP Office Customer Call Reporter Unrestricted File Upload	CVE: 2012-3811 BID: 54225	This strike exploits a flaw in Avaya's IP Office Customer Call Reporter where an unauthenticated user can upload an arbitrary file.
Strike WordPress Plugin Quick Post Widget 1.9.1 Cross-site scripting	CWE: 79 CVE: 2012-4226 BID: 54311	WordPress Quick Post Widget plugin contains multiple cross-site scripting vulnerabilities.
Strike Symantec Messaging Gateway Information Disclosure	CWE: 22 CVE: 2012-4347 BID: 56789	This strike exploits one of two directory traversal vulnerabilities exist in Symantec Messaging Gateway. The vulnerabilities are cause by improper validation of user-supplied input, specifically HTTP parameters. A remote attacker could exploit these vulnerabilities to download arbitrary system files.
Strike HP Intelligent Management Center Arbitrary File Upload	CVE: 2012-5201 BID: 58385	This strike exploits a flaw in HP's Intelligent Management Center where a user can upload a zip file which in turn clobbers arbitrary files.
Strike Adobe Flash Player Memory Corruption	CWE: 119 CVE: 2012-5271	This strike exploits a flaw in Adobe's Flash Player where a malformed action script can write variables which are not allocated and leads to memory corruption.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Movable Type 4.2x, 4.3x Upgrade Script RCE	CWE: 287  CVE: 2013-0209  CVE: 2012-6315	This strike exploits Movable Type 4.2x, 4.3x upgrade script to gain remote code execution on target server.
Strike SonicWall Multiple Products setSessionCheck Authentication Bypass	CVE: 2013-1359  BID: 57445	This strike exploits a vulnerability that is present in multiple SonicWall products and that allows remote unauthenticated access. The vulnerability is located at the level of the applianceMainPage
Strike PHP php_quot_print_encode parameter parsing heap buffer overflow	CWE: 119  CVE: 2013-2110  BID: 60411	This strike exploits a buffer overflow vulnerability in PHP. When parsing percent encoded parameters, specially crafted strings can cause a heap buffer overflow. Successful exploitation may allow arbitrary code execution or abnormal termination of application using php, resulting in a denial of service condition.
Strike Apache Struts URL Command Execution	CWE: 94  CVE: 2013-2115  BID: 60167	This strike exploits command execution vulnerability in Apache Struts. A specially crafted URL can be sent to enable allowStaticMethodAccess and execute arbitrary Java runtime commands. Successful exploitation can result in execution of arbitrary code.
Strike Apache Struts OGNL action-redirect-redirectAction Command Execution	CWE: 20  CVE: 2013-2251  BID: 61189	This strike exploits command execution vulnerability in Apache Struts. A specially crafted HTTP GET or POST requests can be sent to the Apache Struts server to execute arbitrary code with user privileges.
Strike HP System Management Homepage iprange Stack Buffer Overflow	CWE: 121  CVE: 2013-2362	A stack buffer overflow exists in HP System Management Homepage. The vulnerability is due to insufficient input validation when handling HTTP requests containing an iprange variable to the /proxy/DataValidation URI. A remote unauthenticated attacker could exploit this vulnerability by sending a crafted request to the vulnerable service. Successful exploitation could result in arbitrary code execution in the context of the currently affected service, which is System by default.
Strike Oracle Java Final Field Overwrite Remote Code Execution	CWE: 265  CVE: 2013-2423	This strike exploits a design weakness vulnerability in Oracle Java JRE/JDK. This vulnerability is due to improper validation of user supplied input. A remote attacker could exploit this vulnerability by enticing a user to open a crafted webpage and can result in remote code execution in the context of the user running the browser.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle Java java.util.concurrent.ConcurrentHashMap Memory Corruption	CVE: 2013-2426 BID: 59206	This strike exploits a memory corruption vulnerability in Oracle Java. The vulnerability is due to insufficient validation of serialized ConcurrentHashMap objects. Successful exploitation of this vulnerability could result in the execution of arbitrary Java code on the target system.
Strike Squid HTTP Host Header Denial of Service	CWE: 20 CVE: 2013-4123	This strike exploits a vulnerability in Squid Internet Proxy application. If an HTTP request is received, squid parses the host headers looking for a hostname:portnumber. The port number is then used in a conversion, and if this conversion fails the process will terminate.
Strike Symantec Endpoint Protection XXE Injection	CVE: 2013-5014 BID: 65466	This strike exploits an XXE injection vulnerability in Symantec Endpoint Protection management console. This vulnerability is due to improper handling XML external entities in the management console. A remote attacker can take advantage of this vulnerability to do DoS attack on the target system.
Strike WordPress Complete Gallery Manager Plugin Arbitrary File Upload	CVE: 2013-5962	This strike exploits a vulnerability inside the Complete Gallery Manager Plugin for WordPress which allows remote users to upload arbitrary files to the server.
Strike EMC CMCNE FileUploadController Arbitrary File Upload	CWE: 94 CVE: 2013-6810	This strike exploits a EMC Connectrix Manager Converged Network Edition SAN management suite. Due to improper authorization, a remote unauthenticated attacker may upload an arbitrary files through the FileUploadController servlet. All versions of the software prior to 12.0.3 are vulnerable.
Strike Synology DiskStation manager SLICEUPLOAD Remote Command Execution	CWE: 264 CVE: 2013-6955	This strike exploits a vulnerability for Synology Diskstation Manager. Specifically, the exploit targets how user input is processed and appended to files when using the SLICEUPLOAD functionality. The flaw allows an unauthenticated remote attacker to write random command to server side script files and potentially leverage arbitrary command execution. All version belonging to 4.1.x software branch are vulnerable.
Strike Apache HTTP Server mod_status Race Condition Heap Buffer Overflow, verified	CWE: 362 CVE: 2014-0226 BID: 68678	This strike exploits a race condition vulnerability in Apache HTTP Server which leads to a heap buffer overflow. When simultaneously processing requests to server-status and to any other uri, it is possible for a non-null terminated string to be created. The system attempts to copy this until it finds null characters, leading to a heap buffer overflow. Successful exploitation can result in execution of arbitrary code or abnormal termination of the Apache HTTP Server.
Strike Microsoft Internet Explorer Use After Free	BID: 65372 CWE: 119 CVE: 2014-0274	This strike exploits a vulnerability in Microsoft Internet Explorer. If a DOMNodeRemoved event is triggered and all the objects that belong to the current HTMLSelection object are removed inside the event handler for DOMNodeRemoved, a use-after-free condition can occur.

Name	References	Description
Strike Microsoft Internet Explorer Use After Free CVE 2014-0305	CWE: 119 CVE: 2014-0305 BID: 66030	This strike exploits a use after free error triggered when Microsoft Internet Explorer handles DOM rewrites when processing certain web pages. If a user opens a specially crafted web page, on a vulnerable machine, a heap memory corruption is triggered that can lead to arbitrary code execution using local privileges. All versions of Internet Explorer 6 through 11.
Strike Novell GroupWise FileUploadServlet Directory Traversal	CWE: 200 CVE: 2014-0600 BID: 69424	This strike exploits a directory traversal vulnerability in Novell GroupWise. The vulnerability is due to improper validation of user supplied parameters in the fileUpload servlet. An unauthenticated attacker can exploit this vulnerability by sending a specially crafted request to the vulnerable server, leading to the disclosure and destruction of files in arbitrary locations on the server. NOTE: By default the vulnerable services are accessed via SSL connection (port 9710).
Strike WordPress WP Symposium Plugin Arbitrary File Upload	CVE: 2014-10021 BID: 71686	This strike exploits a file upload vulnerability in Wordpress WP Symposium Plugin version 14.11. The vulnerability is due to lack of sanitization of the user-uploaded files in UploadHandler.php. By exploiting this vulnerability, an unauthenticated attacker can execute arbitrary code by uploading files on the server and execute them.
Strike PHP Libmagic Executable PE Selection Table Entry Out of Bounds Memory Access	CWE: 119 CVE: 2014-2270	This strike exploits an out of bounds memory access vulnerability in PHP Libmagic. An executable file with a specially crafted PE selection table entry can cause an integer overflow when calculating the memory address. This will bypass verification, allowing for access of an out of bounds memory location. Successful exploitation can result in execution of arbitrary code or abnormal termination of PHP, resulting in a denial of service condition.
Strike Atlassian Jira Issue Collector Directory Traversal	CWE: 22 CVE: 2014-2314 BID: 65849	This strike exploits a vulnerability in the Atlassian JIRA software suite. It allows a remote unauthenticated attacker to upload a file to random location on the file system by exploiting a directory traversal vulnerability. All versions of JIRA prior to 6.0.3 are vulnerable.
Strike Oracle Event Processing FileUploadServlet filename Parameter Directory Traversal	CVE: 2014-2424 BID: 66871	This strike exploits a directory traversal exploit in Oracle Event Processing. When processing multipart messages sent to FileUploadServlet, the filename parameter is not sanitized for directory traversal characters. Successful exploitation can result in creation or overwrite of arbitrary files.
Strike HP Universal CMDB Default Credentials Arbitrary File Upload	CVE: 2014-2617 BID: 68363	This strike exploits a code execution vulnerability in HP Universal CMDB. The vulnerability is due to the use of hard-coded credentials with administrator rights. By exploiting this vulnerability, an attacker can upload files on the server using the hard-coded credentials and execute code with SYSTEM privileges.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer basefont ASLR Bypass	CWE: 264 CVE: 2014-4140 BID: 70325	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer. An attacker can entice a target to visit an HTML page with a specially crafted basefont tag to trigger the vulnerability. Successful exploitation can result in execution of arbitrary code or abnormal termination of Internet Explorer.
Strike ManageEngine Multiple Products FileAttachment directory traversal	CWE: 22 CVE: 2014-5301	This strike exploits a directory traversal vulnerability in multiple ManageEngine products. The vulnerability is due to improper validation of the path parameter when uploading files to the server. By exploiting this vulnerability, an authenticated attacker can upload files to arbitrary locations on the server and execute them.
Strike ManageEngine Multiple Products multipartRequest Directory Traversal	CWE: 22 CVE: 2014-6036 BID: 70172	This strike exploits a vulnerability inside multiple products from the Manage Engine suite which allows arbitrary file execution. The vulnerability is due to lack of authentication controls and directory traversal vulnerabilities.
Strike ManageEngine EventLog Analyzer agentUpload Directory Traversal	CWE: 22 CVE: 2014-6037 BID: 69482	This strike exploits a code execution vulnerability inside ManageEngine EventLog Analyzer. The vulnerability allows remote unauthenticated attackers to upload files to arbitrary locations and grants execution abilities with System privileges.
Strike Novell Zenworks Configuration Management Rtrlet Directory Traversal	CWE: 22 CVE: 2015-0781 BID: 74291	This strike exploits a directory traversal vulnerability in Novell Zenworks Configuration Management. The vulnerability is due to improper validation of user supplied data in the Rtrlet class when uploading files to the server. By exploiting this vulnerability, an unauthenticated attacker can upload files to arbitrary locations on the server and execute them.
Strike ManageEngine ServiceDesk Plus Privilege Bypass Information Disclosure	CWE: 200 CVE: 2015-1480 BID: 72302	This strike exploits a directory traversal vulnerability in ServiceDesk. A non-administrator user can access certain directories which should be restricted to administrators due to insufficient validation. Successful exploitation can result in disclosure of information.
Strike Oracle Endeca Information Discovery Integrator ETL Server Directory Traversal Vulnerability Through CopyFile	CVE: 2015-2604 BID: 75757	This strike exploits a directory traversal vulnerability in Oracle Endeca Information Discovery Integrator ETL Server. The vulnerability is due to improper validation of parameters when handling CopyFile operation in SOAP requests. An attacker could exploit this vulnerability in order to gain unauthorized access to information or services.

Name	References	Description
Strike Oracle Endeca Information Discovery Integrator ETL Server Directory Traversal Vulnerability Through MoveFile	CVE: 2015-2605 BID: 75756	This strike exploits a directory traversal vulnerability in Oracle Endeca Information Discovery Integrator ETL Server. The vulnerability is due to improper validation of parameters when handling MoveFile operation in SOAP requests. An attacker could exploit this vulnerability in order to gain unauthorized access to information or services.
Strike Wordpress Simple Ads Manager Arbitrary File Upload	CVE: 2015-2825 BID: 73924	This strike exploits a directory traversal vulnerability in Wordpress Simple Ads Manager. The vulnerability is due to lack of sanitization of the path parameter in sam-ajax-admin.php. By exploiting this vulnerability, an unauthenticated attacker can upload arbitrary files on the server and execute them.
Strike TP-Link Archer Devices Directory Traversal	CWE: 22 CVE: 2015-3035	This strike exploits a directory traversal vulnerability in TP-Link Archer Devices. This vulnerability is due to insufficient input validation. A remote, unauthenticated attacker could exploit this vulnerability to read sensitive information from arbitrary files located on the file system of the target server.
Strike PHP tar Zero Length File Name Integer Overflow	CWE: 189 CVE: 2015-4021 BID: 74700	This strike exploits an integer overflow vulnerability in PHP. When PHP processes a tar file, it determines the length of the filename by the displacement of the first null byte. A later calculation subtracts 1 from this length. If the calculated length was zero, the calculation results in an unsigned integer overflow, allowing access to a large portion of the heap. Successful exploitation may result in execution of arbitrary code with privileges of the service running PHP or abnormal termination of the service.
Strike Endian Firewall Proxy Reset Pasword Command Execution	CWE: 77 CVE: 2015-5082 EXPLOITDB : 38096 BID: 76865	This strike exploits a input validation error present in Endian Firewall. Vulnerability can be exploited by crafting a special HTTP request to the target. Successful exploitation would result in arbitrary command execution in the security context of Apache httpd server.
Strike ManageEngine Desktop Central fileupload connectionID Directory Traversal Arbitrary File Upload	CWE: 434 CVE: 2015-8249 EXPLOITDB : 38982	This strike exploits an arbitrary file upload vulnerability in ManageEngine Desktop Central. Files can be uploaded to the target by sending an HTTP POST request to /fileupload with a query parameter action=rds_file_upload. The connectionId parameter is not checked for directory traversal characters. An attacker can send a malicious HTTP POST request to upload an arbitrary file to an arbitrary location on the target system. Successful exploitation may lead to creation or overwriting of arbitrary files, which may lead to execution of arbitrary code with system privileges.
Strike Oracle Application Testing Suite UploadFileUpload Directory Traversal	CVE: 2016-0491 BID: 81169	This strike exploits a directory traversal exploit in Oracle Application Testing Suite. HTTP POST requests to /olt/UploadFileUpload.do do not sanitize for directory traversal characters. An authenticated attacker can send a specially crafted HTTP POST request to upload arbitrary files to any location writable by the Oracle Load Testing service. Note, while this attack requires authentication, it can be paired with the authentication bypass attack, CVE-2016-0492.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Ruby Rails Dynamic Render Directory Traversal	CWE: 22 CVE: 2016-0752	This strike exploits a Directory Traversal vulnerability in the web component of Ruby Rails. The vulnerability is due to unrestricted use of the render method. A remote unauthenticated attacker could exploit this vulnerability by sending a crafted request. Successful exploitation could result in unauthorized file access and leakage of sensitive data.
Strike Advantech WebAccess Dashboard Multiple File Upload Vulnerabilities	CVE: 2016-0854 BID: 80745 EXPLOITDB : 39735	This strike exploits a file upload vulnerability in Advantech WebAccess. WebAccess has several URIs designed to accept image files. These files are not verified, and specially crafted HTTP POST requests can be used to upload any arbitrary file. This includes uploading asp and aspx files, which can then be called to achieve arbitrary asp code execution with the privileges of the IIS service. Successful exploitation may result in creation of arbitrary files and could lead to arbitrary code execution.
Strike PHP phar_parse_pharfile filename_len Integer Overflow	BID: 95774 CWE: 190 CVE: 2016-10159	This strike causes a denial of service in PHP due to a integer overflow when parsing a phar file. The flaw is a bounds check for the filename length field embedded in the file. A malicious file can cause a PHP server to crash.
Strike Adobe Flash Out of Bounds When Placing Object	CVE: 2016-1104 BID: 90618 EXPLOITDB : 39825 GOOGLE: 794	This strike exploits a remote code execution vulnerability in Adobe Flash Player. The vulnerability is due to an out of bounds read when placing a corrupt image. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in abnormal termination of the flash process.
Strike NETGEAR Management System NMS300 File Upload Vulnerability	CVE: 2016-1524 BID: 82630	This strike exploits a file upload vulnerability in NETGEAR Management System NMS300. The vulnerability is due to improper unauthenticated access to certain URLs that allow uploading of files and then accessing them. By exploiting this vulnerability an attacker could upload and execute code on the target machine.
Strike Novell Service Desk LiveTime File Upload Directory Traversal	CWE: 22 CVE: 2016-1593	This strike exploits a directory traversal vulnerability in Novell Service Desk. Service Desk allows administrators to upload CSV files, however Service Desk fails to validate the file is actually a CSV and does not sanitize for directory traversal characters. An authenticated user could exploit this in order to upload arbitrary files to arbitrary locations. Additionally, Service Desk contains default administrator credentials, which could be used by an attacker to gain authentication.

Name	References	Description
Strike GD Library libgd gd_gd2 c Heap Buffer Overflow	CWE: 189 CVE: 2016-3074	A heap buffer overflow vulnerability has been reported in libgd. The vulnerability is due to a signedness error that leads to a heap buffer overflow. Libgd is included within PHP. A remote attacker can exploit this flaw having the target process a crafted malicious GD2 file. Successful exploitation could result in code execution in the security context of the user process.
Strike Adobe Flash ATF Processing Heap Overflow	CVE: 2016-4135 GOOGLE: 786	This strike exploits a remote code execution vulnerability in Adobe Flash Player. The vulnerability is due to a heap overflow in ATF processing. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in execution of arbitrary code or abnormal termination of the flash process.
Strike Symantec Web Gateway Whitelist white_ip Command Execution	CWE: 78 CVE: 2016-5313 BID: 93284	This strike exploits a command execution vulnerability in Symantec Web Gateway. Authenticated requests to the URI / spywall/new_whitelist.php are used to create whitelists. The parameter white_ip is not validated if the sid parameter is non-zero. The value of white_ip will later be used in a shell command, allowing for arbitrary command execution with administrative privileges. An authenticated attacker could send specially crafted HTTP messages to achieve arbitrary command execution with administrative privileges.
Strike WordPress Admin API Directory Traversal	CWE: 22 CVE: 2016-6896	This strike exploits a directory traversal vulnerability inside WordPress. Specifically this occurs when HTTP requests are sent to the admin-ajax page with the action parameter update-plugin set. Directory traversal characters are not handled properly, and an authenticated user can send multiple requests to this API, which will result in a denial of service condition.
Strike Microsoft Edge Browser Chakra Engine Array.map Type Confusion	CWE: 119 CVE: 2016-7190 BID: 93428	This strike exploits a vulnerability in the Microsoft Edge Browser. Specifically, a type confusion vulnerability exists in the Microsoft Edge module Chakra.dll. A malicious attacker can craft javascript in such a way that when a proxy object is created and Array.map is called upon that object, memory information can be disclosed. It may also be possible to cause a denial of service condition in the browser or achieve remote code execution by corrupting these memory contents in a specified manner.
Strike Brocade Network Advisor FileReceiveServlet filename Directory Traversal	CWE: 22 CVE: 2016-8204	This strike exploits a directory-traversal vulnerability in Brocade Network Advisor. The vulnerability is due to lack of input-validation on the filename parameter for FileReceiveServlet. A remote attacker could exploit this vulnerability to upload arbitrary files and result in arbitrary code execution with privileges of the SYSTEM.
Strike Brocade Network Advisor DashboardFileReceiveServlet Directory Traversal Vulnerability	CVE: 2016-8205	This strike exploits a directory traversal vulnerability in Brocade Network Advisor. The vulnerability resides in the DashboardFileReceiveServlet servlet due to insufficient input validation of the filename parameter in HTTP multipart form requests. A remote, unauthenticated attacker could exploit this vulnerability to upload malicious files, potentially leading to arbitrary code execution with SYSTEM privileges.

Name	References	Description
Strike Primetek Primefaces Padding Oracle Remote Code Execution	CWE: 326 CVE: 2017-1000486	This strike exploits a command injection vulnerability in the web component of Primetek Primefaces. The vulnerability is due to inadequate encryption strength. A remote attacker could exploit this vulnerability by sending a crafted request using the known password or the default password. Successful exploitation could result in arbitrary command execution under the security context of the root user.
Strike Synology Photo Station Arbitrary File Upload	CWE: 287 CVE: 2017-11151 EXPLOITDB : 42434	This strike exploits an Arbitrary File Upload vulnerability in Synology Photo Station. The vulnerability is due to improper input validation of user controlled input. A remote, unauthenticated attacker can upload arbitrary files to the target server.
Strike Apache Tomcat Misconfigured HTTP PUT Remote Code Execution	CWE: 434 CVE: 2017-12617	This strike exploits a file upload vulnerability in Apache Tomcat. The vulnerability arises from a misconfiguration in handling PUT requests. When Tomcat is configured with readonly set to false and PUT requests are allowed, attackers can upload files with names ending in ".jsp///". Tomcat removes the trailing slashes, saving the file as a ".jsp" that includes attacker-controlled data. A remote, unauthenticated attacker can exploit this vulnerability by sending a PUT request with a malicious payload in the .jsp file, which executes when accessed. Successful exploitation could result in remote code execution within the context of the user running the Apache Tomcat.
Strike Cacti spikekill php Cross-Site Scripting	CWE: 79 CVE: 2017-12927	This strike exploits a reflected cross-site scripting vulnerability in Cacti. This vulnerability is due to improper validation of the method parameter within spikekill.php. The method value should be one of the stddev, float, variance, or fill. A remote attacker could exploit this vulnerability by enticing an authenticated user to visit a maliciously crafted URL in which the value of method is not one of the previously mentioned values. Successful exploitation could lead to arbitrary script code execution in the context of the user's browser.
Strike Apache httpd FilesMatch Policy Bypass	CWE: 20 CVE: 2017-15715 BID: 103525	This strike exploits a policy bypass vulnerability in Apache httpd FilesMatch. FilesMatch is intended to prevent files which do not match certain regex patterns to be uploaded via HTTP PUT messages. One of these patterns is AP_REG_DOLLAR_ENDONLY, which is intended to prevent files ending with the character. However, this option does not work properly, allowing for files ending with to be uploaded. An attacker can send a specially crafted HTTP PUT message to bypass the policy and upload arbitrary files.
Strike Palo Alto Networks Management Interface Authentication Bypass	CVE: 2017-15944 EXPLOITDB : 43342 BID: 102079	This strike exploits a management interface authentication bypass vulnerability in Palo Alto Networks PAN-OS 6.1.18 and earlier, PAN-OS 7.0.18 and earlier, and PAN-OS 7.1.13 and earlier. Note: A remote user can exploit a combination of vulnerabilities in the management interface to execute arbitrary commands on the target system. The code will run with root privileges. This strike simulates panAuthCheck authentication bypass.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike NetGain Systems Enterprise Manager settings.upload filename Directory Traversal	CWE: 668 CVE: 2017-16603 BID: 102307	This strike exploits a vulnerability in NetGain Systems Enterprise Manager prior to v7.2.766. The vulnerability is caused by insufficient validation of user input in http requests. Successful exploitation could result in arbitrary file accessible on target server.
Strike Roundcube Webmail timezone File Disclosure Vulnerability	CWE: 552 CVE: 2017-16651	This strike exploits Local File Inclusion vulnerability in Roundcube webmail. The vulnerability occurs due insufficient input validation in conjunction with the file-based attachment plugins. An authenticated remote attacker with an active session can exploit this vulnerability by sending crafted request to the server. Successful exploitation of this vulnerability leads to information disclosure by accessing arbitrary files
Strike Advantech WebAccess SCADA gmicons.asp Arbitrary File Upload	CWE: 434 CVE: 2017-16736	An arbitrary file overwrite vulnerability has been identified in Advantech WebAccess SCADA web platform. The vulnerability is caused by the lack of proper input sanitisation of the gmicons.asp picfile parameter. The vulnerability can be exploited by sending a specially-crafted request, allowing the attacker to execute code on the remote machine with the privileges of the application process.
Strike Quest NetVault Backup NVBUEventHistory SQL Injection	CWE: 89 CVE: 2017-17412 BID: 102252	An SQL injection vulnerability exists in Quest NetVault Backup appliance. The vulnerability is due to insufficient user-supplied input validation within Server Process Manager Service. The successful exploitation of this vulnerability can result in database information disclosure without authentication via a specially crafted HTTP request.
Strike Quest NetVault Backup NVBUTransferHistory SQL Injection	CWE: 89 CVE: 2017-17419	An SQL injection vulnerability exists in Quest NetVault Backup appliance. The vulnerability is due to insufficient user-supplied input validation within Server Process Manager Service. The successful exploitation of this vulnerability can result in database information disclosure without authentication via a specially crafted HTTP GET request.
Strike Quest NetVault Backup NVBUJobCountHistory SQL Injection	CWE: 89 CVE: 2017-17420 BID: 102252	An SQL injection vulnerability exists in Quest NetVault Backup appliance. The vulnerability is due to insufficient user-supplied input validation within Server Process Manager Service. The successful exploitation of this vulnerability can result in database information disclosure without authentication via a specially crafted HTTP request.
Strike Oracle Fusion Middleware MapViewer Code Execution	CVE: 2017-3230 BID: 97746	This strike exploits a Code Execution vulnerability in the Oracle Fusion Middleware MapViewer component of Oracle Fusion Middleware. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data.

Name	References	Description
Strike Oracle WebLogic Server OS Command Injection Vulnerability	CWE: 78 CVE: 2017-3506	This strike exploits an OS command injection vulnerability in Oracle WebLogic Server. The vulnerability is caused by insecure deserialization of untrusted data. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted serialized object to the vulnerable WebLogic Server. When the server processes this object, it deserializes the data, leading to the execution of the attacker's code.
Strike HPE Intelligent Management Center UrlAccessController Authentication Bypass	CWE: 287 CVE: 2017-5791	This strike exploits an authentication bypass vulnerability in HPE Intelligent Management Center. This vulnerability is due to doFilter method which contains multiple ways to bypass authentication if the URI contains specific strings. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target system. Successful exploitation allows to bypass authentication requirements, which can be leveraged to execute arbitrary code in the context of SYSTEM.
Strike NETGEAR DGN2200 Devices OS Command Injection Vulnerability	CVE: 2017-6334 CWE: 78	This strike exploits an OS command injection vulnerability on NETGEAR DGN2200 routers. The vulnerability is due to improper input validation in user-supplied input , allowing shell metacharacters in the host_name field of an HTTP POST request in dnslookup.cgi script. A remote authenticated attacker can exploit this by sending a crafted POST request with valid login details. Successful exploitation could allow the attacker to execute arbitrary OS commands on the device.
Strike Apache HTTP Server Token Out of Bounds Read	CWE: 20 CVE: 2017-7668 BID: 99137	This strike exploits a denial of service vulnerability in Apache HTTP Server. The vulnerability is due to an out-of-bounds that read exists in Apache when handling HTTP request with a malicious connection header field. By maliciously crafting a sequence of request headers, an attacker may be able to cause a DoS attack.
Strike PHP gdImageCreateFromGifCtx Out Of Bound Read	CWE: 200 CVE: 2017-7890 BID: 99492	This strike exploits a PHP information disclosure vulnerability before version 5.6.31 and 7.x before 7.1.7 . This vulnerability is due to improper handling of objects in memory under GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c file. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted image file to the target server. Successful exploitation results in information disclosure.
Strike Exponent CMS eaasController php api Function SQL Injection	CWE: 89 CVE: 2017-7991	This strike exploits an SQL injection vulnerability in Exponent CMS. The vulnerability is due to a lack of input validation on the apikey HTTP parameter by the api() function. A remote, unauthenticated user can exploit this vulnerability by sending a crafted HTTP request to the affected page. Successful exploitation could result in the execution of arbitrary SQL commands on the target server.

Name	References	Description
Strike HPE Intelligent Management Center flexFileUpload Arbitrary File Upload	CWE: 22 CVE: 2017-8961	This strike exploits an arbitrary file upload vulnerability in Hewlett Packard Enterprise (HPE) Intelligent Management Center. By design, the uri /imc/flexFileUpload should accept xml documents in multipart/form-data encoding. However, file extension and type are not validated, allowing for arbitrary file upload. An attacker can send specially crafted HTTP POST requests containing an arbitrary file with multipart/form-data to upload the file. If the file is of type .jsp or .jspx, the attacker can then request the file to achieve arbitrary code execution with SYSTEM privileges.
Strike PHPUnit Command Injection	CWE: 94 CVE: 2017-9841	This strike exploits a command injection vulnerability in PHPUnit. This vulnerability lies within the /phpunit/src/Util/PHP/eval-stdin.php file through its use of the php://input wrapper. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted post request to the target server. Successfully exploiting this vulnerability could result in arbitrary PHP code execution on the target system.
Strike Trend Micro Endpoint Application Control FileDrop Directory Traversal	CWE: 22 CVE: 2018-10357	This strike exploits a directory traversal vulnerability in the management console of Trend Micro Endpoint Application Control. The vulnerability is due to insufficient validation of filenames in the filename parameter of the Content-Disposition header in multipart/form-data requests sent to FileDropService. A remote, authenticated user can exploit this vulnerability by submitting a crafted request to the target server. Successful exploitation could result in the execution of arbitrary code as the SYSTEM user.
Strike Quest KACE System Management Appliance Remote Code Execution	CWE: 78 CVE: 2018-11138	This strike exploits a critical command injection vulnerability within the Quest KACE System Management Appliance. The vulnerability arises from the /common/download_agent_installer.php script's inadequate sanitization of user-supplied input. Specifically, arises due to the the script fails to properly neutralize special elements used in operating system commands, allowing an attacker to inject arbitrary commands. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the vulnerable endpoint, potentially leading to remote code execution.
Strike Quest Appliance - NetVault Backup Stack Buffer Overflow	CWE: 20 CVE: 2018-1161	A stack buffer overflow has been identified in Quest NetVault Backup appliance. The vulnerability is caused by the lack of proper input sanitisation in the context of multipart HTTP requests processing. The vulnerability can be exploited by accessing the Web Interface of the NetVault server via a specially-crafted HTTP POST request, allowing the attacker arbitrary code execution with SYSTEM privileges.
Strike Quest Appliance - NetVault Backup Arbitrary File Overwrite	CVE: 2018-1162	An arbitrary file overwrite vulnerability has been identified in Quest NetVault Backup appliance. The vulnerability is caused by the lack of user input sanitisation in the context of log exportation. The vulnerability can be exploited by accessing the Web Interface of the NetVault server via a specially-crafted HTTP POST request, allowing the attacker to overwrite any file with SYSTEM privileges.
Strike Quest NetVault Backup Checksession Authentication Bypass	CVE: 2018-1163	This strike exploits an authentication bypass vulnerability in Quest NetVault Backup. The vulnerability is due to insufficient validation of the checksession parameter in multipart HTTP requests. Successful exploitation may result in successful bypass of the authentication mechanism.

Name	References	Description
Strike Mozilla Firefox Javascript Array.Prototype.Push Information Disclosure	CWE: 20 CVE: 2018-12387 BID: 105460	This strike exploits an information disclosure vulnerability in the Mozilla Firefox browser. Specifically, the JavaScript JIT compiler inlines Array.prototype.push with multiple arguments that result in the stack pointer being off by 8 bytes. When this occurs a memory address gets leaked that can be used as part of an exploit. This strike demonstrates the information disclosure by dumping the leaked memory addresses.
Strike Apache Pluto PortletV3Annotated Demo MultipartPortlet Arbitrary File Upload	CWE: 200 CVE: 2018-1306 EXPLOITDB : 45396	A file upload vulnerability was found in Apache Pluto PortletV3AnnotatedDemo. The vulnerability is due to improper access control of user-supplied input when the portlet performs a file-uploading operation. Successful exploitation can result arbitrary file upload and possible remote code execution in the context of the user running the webserver.
Strike Fortinet FortiOS and FortiProxy SSLVPN Web Portal Magic Improper Authorization	CVE: 2018-13382 CWE: 863	This strike exploits an improper authorization vulnerability in SSLVPN web portal of Fortinet FortiOS and FortiProxy. The vulnerability is due to improper authorization of the SSL VPN web portal component in FortiOS and FortiProxy. A remote, unauthenticated attacker could exploit this vulnerability by crafting a HTTP request containing a parameter called "magic" with the value "4tinet2095866". Successful exploitation could allow the attacker to modify the password of SSL VPN web portal in Fortinet FortiOS and FortiProxy.
Strike Xen Project XAPI Update Directory Traversal	CWE: 22 CVE: 2018-14007	This strike exploits a directory traversal vulnerability in the XAPI component of Xen. The vulnerability is due to insufficient handling of URL-encoded path components in requests sent to the pool update endpoint, used for supplying updates to other members of a resource pool. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation results in the disclosure of arbitrary file contents from the server, which may include the administrator token.
Strike OpenEMR manage_site_files Unrestricted File Upload	CWE: 434 CVE: 2018-15139	A file upload vulnerability was found in the OpenEMR. The vulnerability is caused by the lack of proper input sanitisation passed to the manage_site_files Web PHP form. Successful exploitation can result in arbitrary code execution in the context of the user running OpenEMR.
Strike Adobe ColdFusion CKEditor upload.cfm Directory Traversal	CWE: 20 CVE: 2018-15960 BID: 105317	This strike exploits a directory traversal vulnerability in Adobe ColdFusion CKEditor. The vulnerability is due to improper sanitization in the file upload.cfm. An attacker could exploit this vulnerability by sending a crafted HTTP request to the target server. By successfully exploiting this vulnerability, a remote, unauthenticated attacker could upload arbitrary files to the target server.
Strike Adobe ColdFusion CKEditor upload.cfm Unrestricted File Upload	CWE: 434 CVE: 2018-15961	This strike exploits an unrestricted file upload vulnerability in Adobe ColdFusion CKEditor. The vulnerability is due to improper restrictions on the files uploaded by users. By successfully exploiting this vulnerability, an remote, unauthenticated attacker could upload arbitrary files and execute them on the target server.

Name	References	Description
Strike LimeSurvey TCPDF phar Deserialization Remote Code Execution	CWE: 502 CVE: 2018-17057 EXPLOITDB : 46634	This strike exploits a remote code execution in LimeSurvey. The vulnerability resides in a PHP Phar deserialization within the 'TCPDF' component and can be exploited by uploading a malicious JPEG/Phar polyglot and exporting the survey that contains it. Exploiting this flaw requires authentication and results in remote code execution.
Strike MyBB Post Video Stored Cross Site Scripting	CWE: 79 CVE: 2018-17128	This strike exploits a stored cross site scripting vulnerability in MyBB platform. The vulnerability can be exploited by crafting a malicious video attachment when creating a new topic. By exploiting this flaw, an attacker obtains client-side Javascript code execution within victim's browser which can lead to information disclosure and credentials theft.
Strike Webmin history Parameter Cross-Site-Scripting	CWE: 79 CVE: 2018-19191	This strike exploits a cross-site scripting vulnerability in Webmin. The vulnerability results from the lack of sanitization when displaying the POST parameter 'history' in '/shell/index.cgi'. A successful exploitation leads to arbitrary code execution in visitors' browsers or credentials theft.
Strike phpMyAdmin Local File Inclusion	CWE: 200 CVE: 2018-19968	This strike exploits a remote file inclusion vulnerability in phpMyAdmin. The vulnerability is due to an improper filter, and the ability to execute a SQL sentence. By successfully exploiting this vulnerability, a remote, authenticated attacker could retrieve arbitrary files from the target server.
Strike Zoho ManageEngine OpManager SQL Injection in getGraphData API	CVE: 2018-20173	This strike exploits a SQL injection vulnerability in Zoho ManageEngine OpManager. The vulnerability resides in the getGraphData API due to insufficient validation of input parameters such as name, index, and policyName. Exploiting this flaw allows a remote, authenticated attacker to execute arbitrary SQL commands on the application's database, potentially compromising its integrity and security.
Strike Oracle WebLogic Remote Diagnosis Assistant rda_tfa_hrs Command Injection	CWE: 78 CVE: 2018-2616	This strike exploits a command injection vulnerability in the web console of the Oracle WebLogic Remote Diagnosis Assistant. The vulnerability is due to improper input validation of HTTP parameter hrs_since menu command in the Java class OsUtils, the command string is not properly sanitized for command injection characters. A remote authenticated attacker can exploit this vulnerability by sending a crafted request to the target application. Successful exploitation could lead to arbitrary command execution on the target server with privileges of the Administrator user.
Strike Oracle WebLogic Server Fusion Middleware File Upload	CVE: 2018-2894	A file upload vulnerability was found in the Oracle WebLogic Server component of Oracle Fusion Middleware. The vulnerability is caused by the lack of proper input sanitisation of the Weblogic Web Service Test Page. Successful exploitation can result in arbitrary code execution in the context of the user running WebLogic.

Name	References	Description
Strike Trend Micro Control Manager sCloudService GetPassword SQL Injection	CWE: 89 CVE: 2018-3604	This strike exploits an SQL injection vulnerability in the Trend Micro Control Manager. The vulnerability is due to a lack of authentication for accessing the GetPoliciesOfProductType operation and a failure to sanitize the account parameter in the HTTP request. An external, unauthenticated attacker can leverage this vulnerability by sending a crafted HTTP request to the targeted server. Successfully exploiting this vulnerability may result in the execution of arbitrary SQL code within the context of the Network Service user.
Strike Apple Safari WebKit hoistSloppyModeFunctionIfNecessary Improper Object Validation	CWE: 119 CVE: 2018-4386 GOOGLE: 1665	This strike exploits a vulnerability in Apple Safari Webkit. Specifically the vulnerability exists in the BytecodeGenerator::hoistSloppyModeFunctionIfNecessary method. It is possible to craft Javascript in such a way that allows for an object to be passed as the property variable directly as a string to the op_get_direct_pname handler without being properly validated. This can lead to a denial of service in the browser application or potentially allow for remote code execution to occur.
Strike Advantech WebAccess SCADA certUpdate.asp Directory Traversal	BID: 102781 CWE: 22 CVE: 2018-5445	An arbitrary file overwrite vulnerability has been identified in Advantech WebAccess SCADA web platform. The vulnerability is caused by the lack of proper input sanitisation of the certUpdate.asp filename parameter. The vulnerability can be exploited by sending a specially-crafted request, allowing the attacker to execute code on the remote machine with the privileges of the application process.
Strike Joomla! Hathor Postinstall Message SQL Injection	CWE: 89 CVE: 2018-6376 BID: 102916	This strike exploits an SQL injection vulnerability in Joomla! CMS. The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure, database corruption, denial of service and others.
Strike Schneider Electric IIoT Monitor Zip Directory Traversal	CWE: 434 CVE: 2018-7836	This strike exploits a directory traversal vulnerability in Schneider Electric IIoT Monitor. The vulnerability is due to insufficient handling of directory traversal characters in uploaded ZIP archives uploaded to several endpoints - ProtectionMgmt, RecoveryMgmt, and UpgradeMgmt. An authenticated attacker can exploit this weakness by uploading a crafted ZIP file, allowing them to traverse directories and write arbitrary files to locations accessible by SYSTEM. This vulnerability poses a significant risk of arbitrary code execution.
Strike Apache Superset Import Dashboards Remote Code Execution	CWE: 502 CVE: 2018-8021 EXPLOITDB : 45933	A remote code execution exists in Apache Superset through the 'Import Dashboards' feature. The vulnerability exists as a result of an insecure 'pickle' deserialization, allowing execution of arbitrary methods from the Python library. An authenticated attacker can therefore execute arbitrary code on the target system under the user that runs the 'gunicorn' webserver.

Name	References	Description
Strike Zoho ManageEngine OpManager OpManagerFailover Util customerName SQL Injection	CWE: 89 CVE: 2018-9088	This strike exploits an SQL injection vulnerability that exists in ManageEngine OpManager. The vulnerability results from a lack of input validation of the customerName request parameter and a lack of authentication for accessing FailOverHelperServlet servlet. A remote unauthenticated attacker could exploit this vulnerability by sending an HTTP request with a crafted customerName parameter. If the exploitation is successful, the server will execute a maliciously injected SQL statement, which may lead to data tampering in the OpManagerDB backend database and ultimately to the execution of arbitrary code with the privileges of database process.
Strike Jquery File Upload Arbitrary File Upload	CWE: 434 CVE: 2018-9206 EXPLOITDB : 45584 BID: 105679	This strike exploits an arbitrary file upload vulnerability in BlueImp Jquery File Upload widget. The vulnerability is due to the complete lack of server-side authorization or sanitization when handling a file upload. An attacker is thus able to create arbitrary files on the server which in most cases leads to remote arbitrary code execution.
Strike Microsoft Edge Chakra NewScObjectNoCtor Type Confusion	CWE: 119 CVE: 2019-0567 EXPLOITDB : 46203 BID: 106418 GOOGLE: 1702	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that when using the NewScObjectNoCtor or InitProto methods with the SetIsPrototype method of the type handler, a transition to a new type can cause type confusion to occur. This can lead to a denial of service in the browser or potentially lead to remote code execution.
Strike Kentico Unauthenticated Remote Code Execution via Insecure Dot Net Deserialization	CVE: 2019-10068 CWE: 502	This strike exploits an insecure deserialization vulnerability in Kentico. The vulnerability arises due to a failure to validate security headers in the staging service allowing an attacker to bypass authentication and perform arbitrary operation. An unauthenticated remote attacker can trigger insecure deserialization of user-controlled .NET objects, by sending a specially crafted request, leading to remote code execution. A successful attack could result in full compromise of the Kentico instance and underlying server.
Strike Citrix SD WAN SQL Injection	CWE: 89 CVE: 2019-12989	This strike exploits an SQL Injection vulnerability in Citrix SD-WAN. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted http requests containing shell metacharacters in sitename parameter to get_package_file endpoint. Successful exploitation could allow the attacker to achieve remote code execution.

Name	References	Description
Strike OpenEMR ajax_download.php Directory Traversal Vulnerability	CVE: 2019-14530	This strike exploits a directory traversal vulnerability in OpenEMR. The vulnerability is located in the ajax_download.php script, specifically in the improper validation of the fileName parameter. Exploiting this vulnerability allows a remote, authenticated attacker to read or delete arbitrary files on the server, potentially leading to information disclosure or denial-of-service conditions.
Strike Cisco DCNM SecurityManager Hard-Coded Cryptographic Key Authentication Bypass	CVE: 2019-15976	This strike exploits an authentication bypass vulnerability in Cisco Data Center Network Manager. The vulnerability exists due to the use of a hard-coded cryptographic key shared across installations for validating Single Sign-On (SSO) tokens. A remote, unauthenticated attacker could exploit this vulnerability by crafting a valid SSO token, allowing them to bypass authentication and execute arbitrary actions through the SOAP API with administrative privileges.
Strike Cisco Prime Data Center Network Manager Arbitrary File Upload	CWE: 264 CVE: 2019-1620 BID: 108906 EXPLOITDB : 47016	This strike exploits a path traversal vulnerability found in Cisco Data Center Network Manager (DCNM). The vulnerability is due to incorrect permission settings in affected DCNM software. An unauthenticated attacker could exploit this vulnerability by uploading a malicious file to the administrative web interface. A successful exploit could allow the attacker to write arbitrary files on the filesystem and execute code with root privileges on the affected device.
Strike Nostromo nhttpd http_verify Directory Traversal	CVE: 2019-16278 CWE: 22	This strike exploits a directory traversal vulnerability in Nostromo nhttpd server. The vulnerability is due to a failure on part of the http_verify function to properly parse user requests. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation could result in information disclosure and in the worst case, allows the attacker to execute arbitrary system commands under the context of the server process.
Strike WiKID 2FA Enterprise Server SQL Injection in searchDevices.jsp	CVE: 2019-16917	This strike exploits an SQL injection vulnerability in WiKID 2FA Enterprise Server. The vulnerability exists due to improper sanitization of user-supplied input in the searchDevices.jsp file. A remote, authenticated attacker could leverage this flaw by sending specially crafted HTTP requests, potentially leading to the execution of arbitrary SQL commands on the backend database.
Strike WiKID 2FA Enterprise Server processPref.jsp SQL Injection Vulnerability	CVE: 2019-17117	This strike exploits an SQL injection vulnerability in WiKID 2FA Enterprise Server. The vulnerability exists due to improper sanitization of user-supplied input in the processPref.jsp file. A remote, authenticated attacker can leverage this flaw by sending specially crafted HTTP requests, potentially leading to the execution of arbitrary SQL commands on the backend database.

Name	References	Description
Strike Cisco Prime Infrastructure Health Monitor - TarArchive Directory Traversal	CWE: 20 CVE: 2019-1821 BID: 108339 EXPLOITDB : 47016	This strike exploits a path traversal vulnerability found in Cisco Prime Infrastructure (PI) and Cisco Evolved Programmable Network (EPN) Manager. The vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by uploading a malicious file to the administrative web interface. A successful exploit could allow the attacker to execute code with root-level privileges on the underlying operating system.
Strike OpenEMR scanned_notes-new.php OS Command Injection	CWE: 77 CVE: 2019-3968	A command injection vulnerability exists in OpenEMR 5.0.1 and earlier, within 'scanned_notes/new.php' form file, as a result of weak user input sanitization. By sending a crafted 'id' parameter in a HTTP request, a remote authenticated attacker might execute arbitrary system commands.
Strike HPE IMC Expression Language Injection via beanName Parameter	CVE: 2019-5373	This strike exploits an Expression Language injection vulnerability in HPE Intelligent Management Center. The vulnerability exists due to improper validation of the `beanName` parameter in the `CustomReportTemplateSelectBean` class. A remote, authenticated attacker can leverage this flaw to execute arbitrary code on the target system with SYSTEM-level privileges.
Strike HPE Intelligent Management Center Expression Language Injection Vulnerability cve_2019_5385	CVE: 2019-5385	This strike exploits an Expression Language injection vulnerability in HPE Intelligent Management Center. The vulnerability resides in the insufficient validation of the beanName parameter within the perfSelectTask endpoint. Exploiting this flaw allows a remote attacker to execute arbitrary code on the target system under the security context of the SYSTEM user.
Strike Drupal Core Phar Stream Insecure PHP Deserialization	CWE: 20 CVE: 2019-6339	A remote code execution vulnerability exists in Drupal 7.x before 7.62, Drupal 8.5.x before 8.5.9 and Drupal 8.6.x before 8.6.6. The vulnerability is located within the PHP's built-in phar stream wrapper, when performing file operations on an untrusted 'phar://' URI. A remote attacker can exploit this vulnerability by sending a crafted HTTP packet to the target service. Successful exploitation could lead to arbitrary code execution or crash of the vulnerable application.
Strike SonicWall SMA100 SQL Injection Vulnerability	CWE: 89 CVE: 2019-7481	This strike exploits SQL injection vulnerability in SonicWall SMA100. The vulnerability is due to improper neutralization of special elements used in SQL command. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary SQL commands, potentially leading to unauthorized access.
Strike Zoho ManageEngine ServiceDesk Plus Arbitrary File Upload	CWE: 434 CVE: 2019-8394 EXPLOITDB : 46413	This strike exploits a file upload vulnerability in Zoho ManageEngine ServiceDesk Plus. Files can be uploaded to the target by sending an HTTP POST request with a parameter 'module' equal to 'CustomLogin'. An attacker can send a malicious HTTP POST request to upload an arbitrary file to '/custom/login' folder. Successful exploitation may lead to creation and execution of arbitrary files by an authenticated user with minimum permissions (for example, guest).

Name	References	Description
Strike Synacor Zimbra Collaboration Suite Mailboxd Component XXE Vulnerability	CVE: 2019-9670 CWE: 611	This strike exploits an XXE vulnerability in Synacor Zimbra Collaboration Suite. This vulnerability lies in the Mailboxd component. A remote unauthenticated attacker can exploit this vulnerability by crafting a specially crafted XML payload containing malicious code and targeting the Autodiscover/Autodiscover.xml endpoint. Successful exploitation of this vulnerability could lead to data exposure.
Strike Sonatype Nexus Repository Manager ContentSelectorsApi Resource Stored Cross-Site Scripting	CWE: 79 CVE: 2020-10203	This strike exploits a stored cross-site scripting vulnerability in Sonatype Nexus Repository Manager. The vulnerability results from inadequate input validation in the content-selectors REST API request within the Java class ContentSelectorsApiResource. This flaw allows an authenticated attacker to inject malicious script code into the database by sending a carefully crafted request to the target server. Successful exploitation of this vulnerability could lead to the execution of arbitrary code within the security context of the user's browser.
Strike rconfig misconfigured post os command injection	CWE: 78 CVE: 2020-10221	This Strike exploits OS Command Injection Vulnerability against rconfig. The vulnerability is due to Improper Neutralization of elements such as HTTP POST in the configuration. An attacker can exploit this vulnerability by sending OS commands via shell metacharacters in the filename POST parameter. Successful Exploitation would result in the OS command Execution within the context of the user running rconfig.
Strike Advantech WebAccess NMS LicenseImportAction Arbitrary File Upload Vulnerability	CVE: 2020-10621	This strike exploits an arbitrary file upload vulnerability in Advantech WebAccess NMS. The vulnerability resides in the insufficient validation of file paths within the licenseImportAction.action endpoint. A remote, unauthenticated attacker could leverage this flaw to upload malicious files, potentially leading to arbitrary code execution under the SYSTEM user context.
Strike Advantech WebAccess NMS download.jsp Directory Traversal Vulnerability	CVE: 2020-10631	This strike exploits a directory traversal vulnerability in Advantech WebAccess NMS. The vulnerability is located in the download.jsp endpoint, where insufficient input validation is performed on the filename parameter. Exploiting this vulnerability allows a remote, unauthenticated attacker to read or delete arbitrary files on the target server, potentially leading to sensitive information disclosure or denial of service.
Strike rConfig search.crud.php OS Command Injection	CVE: 2020-10879 CWE: 74	This strike exploits a OS Command Injection vulnerability in the rConfig server. The vulnerability is in the 'nodeId' parameter in the 'search.crud.php' module, due to failure to properly sanitize the user-supplied input. A remote, authenticated attacker can create a malicious HTTP request resulting in arbitrary command execution on the target system with the privileges of the user running the web server.

Name	References	Description
Strike Apache Airflow Command Injection	CWE: 78 CVE: 2020-11978	This strike exploits remote code/command injection vulnerability in Apache Airflow. This vulnerability was discovered in one of the example DAGs(Directed Acyclic Graph) shipped with Airflow which would allow any user to run arbitrary commands as the user running airflow worker/scheduler(depending on the executor in use). A remote unauthenticated attacker can exploit this vulnerability by sending a crafted request to apache airflow. *NOTE: When running this strike in OneArm mode, first it searches for the example_trigger_target_dag on the target server. If found, then it unpauses the example dag and then creates a DAG(it is a collection of all the tasks that one may want to run), which in this case is creation of a file /tmp/test .
Strike rConfig vendors.crud.php Arbitrary File Upload Vulnerability	CVE: 2020-12255	This strike exploits an arbitrary file upload vulnerability in the rConfig Network Device Configuration Tool. The vulnerability resides in the improper validation of the HTTP multipart/form-data request parameter vendorLogo within the vendors.crud.php script. Exploiting this vulnerability allows a remote authenticated attacker to upload malicious files, potentially leading to arbitrary code execution under the security context of the affected service.
Strike rConfig Network Device Configuration Tool devicemgmt.php Cross-Site Scripting	CWE: 79 CVE: 2020-12256	This strike exploits a cross-site scripting vulnerability in rConfig Network Device Configuration Tool. The vulnerability is due to improper validation of the user-supplied request parameter deviceId by devicemgmt.php. A remote attacker could exploit this vulnerability by enticing a victim to open a link or a web page. Successful exploitation could result in the execution of script code in security context of the target users browser.
Strike rConfig Network Device Configuration Tool configDevice.php Cross-Site Scripting	CWE: 79 CVE: 2020-12259	This strike exploits a cross-site scripting vulnerability in rConfig Network Device Configuration Tool. The vulnerability arises from inadequate validation of the 'rid' request parameter in configDevice.php. A remote attacker could exploit this vulnerability by enticing a victim to open a link or a web page. If successfully exploited, this could lead to the execution of script code within the security context of the targeted user's browser.
Strike Roundcube Webmail im_convert_path RCE Vulnerability	CWE: 78 CVE: 2020-12641	This strike exploits remote code execution vulnerability in Roundcube webmail. The vulnerability is due to the im_convert_path configuration setting, which allows a remote, unauthenticated attacker with access to the Roundcube installer to inject system commands. These commands execute whenever a user opens an email containing a "non-standard" image. Successful exploitation could lead to arbitrary command execution.
Strike Centreon RRDdatabase_status_path Command Injection Vulnerability	CVE: 2020-13252	This strike targets a command injection vulnerability in the Centreon Web Application. The issue arises from improper validation of the `RRDdatabase_status_path` parameter in HTTP requests. Exploiting this flaw allows a remote, authenticated attacker to execute arbitrary commands on the server with the privileges of the web server process.

Name	References	Description
Strike Apache Kylin REST API Command Injection Vulnerability	CVE: 2020-13925	This strike exploits a command injection vulnerability in Apache Kylin. The vulnerability resides in the diag REST API endpoint, specifically in the DiagnosisService class, where user-supplied input is insufficiently validated. An authenticated remote attacker could leverage this flaw by sending crafted HTTP requests, leading to arbitrary command execution on the server.
Strike Apache OpenMeetings NetTest Denial of Service	CWE: 835 CVE: 2020-13951	This strike exploits a denial of service vulnerability in Apache OpenMeetings 4.0.0 - 5.0.0. The vulnerability is caused by a lack of rate limiting on NetTest. A remote, unauthenticated attacker can send a large number of requests to the server resulting in network exhaustion and denial of service.
Strike Oracle Business Intelligence Enterprise Edition Path Traversal	CWE: 22 CVE: 2020-14864	This strike exploits a directory traversal vulnerability in Oracle Business Intelligence Enterprise Edition. This vulnerability is due to the getPreviewImage function which is used to get the preview image of a previously uploaded theme logo. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request by manipulating the previewFilePath URL parameter. Successful exploitation of this vulnerability could allow an attacker to read sensitive files, execute arbitrary code, or gain unauthorized access to the system.
Strike Ivanti MobileIron Remote Code Execution Vulnerability	CWE: 706 CVE: 2020-15505	This strike exploits a remote code execution vulnerability in MobileIron products. The vulnerability exists in a Tomcat Web Service that deserializes user input using the Hessian format. This unsafe deserialization allows malicious input to be executed, leading to potential remote code execution. Attackers can leverage the inconsistency between Apache and Tomcat to bypass access controls and execute malicious payloads by exploiting deserialization vulnerabilities in the Hessian format. Successful exploitation of this vulnerability could allow a remote, unauthenticated attacker to execute arbitrary code on the affected system.
Strike Microsoft Exchange Server DlpUtils AddTenantDlpPolicy Remote Code Execution	CWE: 94 CVE: 2020-16875	A remote code execution vulnerability exists in Microsoft Exchange Server due to improper validation of cmdlet arguments. A remote authenticated attacker can exploit this vulnerability by running a particular cmdlet with crafted arguments against a vulnerable Exchange server. Successful exploitation could result in the execution of arbitrary commands as SYSTEM.
Strike Fuel CMS Col Parameter SQL Injection Vulnerability	CWE: 89 CVE: 2020-17463	This strike exploits an SQL injection vulnerability in Fuel CMS. This vulnerability lies in the parameter col in permission/items, logs/items, pages/items, navigation/items. An authenticated attacker can exploit this vulnerability by crafting a specially crafted SQL payload. Successful exploitation of this vulnerability could lead to unauthorized access, data leakage and data manipulation.
Strike Apache Flink FileUploadHandler Arbitrary File Upload	CWE: 22 CVE: 2020-17518	This strike exploits a file upload vulnerability in Apache Flink. The vulnerability is due to insufficient input validation while uploading files in the FileUploadHandler class. A remote, unauthenticated attacker can exploit this vulnerability by submitting a crafted request to the target server results in the writing of an arbitrary file to any location writable by the target server. *NOTE: When running this strike in OneArm mode, a randomly generated file is uploaded in the /tmp directory of the target machine .

Name	References	Description
Strike PHP-Fusion Downloads.php Command Injection	CWE: 269 CVE: 2020-24949	This strike simulates a command injection vulnerability in PHP-Fusion. The vulnerability is due to insufficient validation of HTTP request parameters in downloads.php. A remote unauthenticated attacker could exploit this vulnerability by sending an crafted HTTP request to the vulnerable server. Successful exploitation of this vulnerability could allow the attacker to execute command in the security context of the running server.
Strike Advantech R-SeeNet device_position.php SQL Injection Vulnerability	CVE: 2020-25157	This strike exploits a SQL injection vulnerability in Advantech R-SeeNet. The vulnerability exists due to insufficient validation of the device_id parameter in the device_position.php file. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted HTTP requests, potentially leading to the retrieval of sensitive information from the database.
Strike WordPress File Manager connector_minimal.php Improper Access Control	CWE: 434 CVE: 2020-25213	This strike exploits an improper access control vulnerability in the File Manager plugin for WordPress. The vulnerability arises from inadequate access control for the connector_minimal.php file during file uploads. This allows an unauthenticated attacker to upload arbitrary files, including potentially malicious PHP files, posing a risk of executing arbitrary code. A remote, unauthenticated attacker could exploit this vulnerability by submitting a carefully crafted request to a WordPress server with the File Manager Plugin installed. Successful exploitation could lead to the unauthorized upload of arbitrary files, potentially resulting in the execution of arbitrary code within the security context of the WordPress server.
Strike Cisco Security Manager AuthTokenServlet Insecure Deserialization	CWE: 502 CVE: 2020-27131	The strike exploits an insecure deserialization vulnerability in Cisco Security Manager. The vulnerability is due to insufficient validation of serialized data, passed via HTTP(S) request to /CSCOnm/servlet/com.cisco.nm.cmf.servlet.AuthTokenServlet, causing deserialization of untrusted data while having exploitable libraries in the code path. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted serialized object to the target server. Successful exploitation can result in arbitrary code execution as root.
Strike Zyxel Products Use of Hard-Coded Credentials	CWE: 522 CVE: 2020-29583	This strike exploits an use of Hard-Coded Credentials Vulnerability in Zyxel Multiple Products. This vulnerability is due to an undocumented account (zyfwp) with an unchangeable password. The account is designed to deliver automatic firmware updates to connected access points through FTP. A remote, unauthenticated attacker could exploit this vulnerability to gain unauthorized access to the affected device, potentially leading to further compromise of the network.
Strike Cisco UCS Director ApplianceStorageUtil Directory Traversal	CWE: 22 CVE: 2020-3239	A directory traversal vulnerability exists in Cisco UCS Directory. The vulnerability is due to insufficient validation of user input within 'ApplianceStorageUtil' class. A remote authenticated attacker can exploit the vulnerability by sending malicious requests to the target server. Successful exploitation could result in the arbitrary file write and remote code execution under the security context of web server.

Name	References	Description
Strike Cisco UCS Director Directory Traversal Vulnerability	CVE: 2020-3251	This strike exploits a directory traversal vulnerability in Cisco UCS Director. The vulnerability exists due to insufficient validation of user input within the MyCallable class when processing file upload requests. A remote authenticated attacker could leverage this flaw to write arbitrary files to the server, potentially leading to remote code execution under the web server's security context.
Strike Nagios XI Manage Plugins Command Injection	CWE: 78 CVE: 2020-35578	This strike exploits a command injection vulnerability in the admin webpage 'monitoringplugins.php' script for Nagios XI. The flaw is due to the insufficient validation of the 'uploadedfile' multipart filename. The flaw may be exploited by an authenticated attacker to execute arbitrary code in the context of the Nagios user on the target server.
Strike Webmin Package Updates update.cgi Command Injection	CWE: 78 CVE: 2020-35606	This strike exploits a command injection vulnerability in Webmin. The vulnerability is due to the insufficient validation of input in the Package Updates module. A remote attacker could exploit this vulnerability by sending a crafted request to the target system. Successful exploitation of this vulnerability could result in arbitrary command execution on the target system.
Strike OpenEMR Backup php Command Injection	CWE: 78 CVE: 2020-36243	This strike exploits a command injection vulnerability in OpenEMR. This vulnerability is due to insufficient sanitation for the user-supplied data in the backup.php. A remote authenticated attacker can exploit this vulnerability by sending crafted requests to the target server. Successful exploitation could result in arbitrary command execution in the security context as web server. *NOTE: When running this strike in OneArm mode, the requests will not be sent to /openemr/someuri , instead will be sent to /someuri , since the openemr server docker used, is configured that way.
Strike VMware Multiple Products ApplianceSslCertificateService Command Injection	CWE: 77 CVE: 2020-4006	This strike exploits a command injection vulnerability in VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector. The vulnerability is due to improper validation of user input in the 'san' parameter. The flaw may be exploited by an authenticated attacker to execute arbitrary code in the context of the service running on the target server.
Strike IBM Spectrum Protect Plus uploadHttpsCertificate Command Injection	CVE: 2020-4241 CWE: 78	This strike exploits a command injection vulnerability in IBM Spectrum Protect Plus. The vulnerability is due to a lack of input sanitization for injection or invalid characters in the filename parameter. When an attacker sends an HTTP POST request to the "/emi/api/uploadhttpscertificate" URI, command execution can occur.
Strike Ruby on Rails locals render Remote Code Execution	CWE: 94 CVE: 2020-8163	A remote code execution vulnerability exists in Ruby on Rails versions 5 < 5.0.1 and 4 < 4.2.11.2, due to lack of user input validation. The vulnerability manifests itself whenever the 'locals' value for a 'render' call is set to 'params' value. Remote attackers may exploit applications containing the up-mentioned pattern by sending a crafted HTTP request to obtain arbitrary code execution.

Name	References	Description
Strike Squid Reverse Proxy Host Header Buffer Overflow	CWE: 119 CVE: 2020-8450	A stack-based buffer overflow vulnerability exists in Squid before 4.10 due to incorrect buffer management, when acting as a reverse proxy. By sending a crafted HTTP request with a host string longer than 255 characters in the 'Host' header, a remote attacker may achieve remote code execution on the target host.
Strike Trend Micro Apex One and OfficeScan Directory Traversal CVE 2020-8599	CWE: 434 CVE: 2020-8599	This strike exploits a directory traversal vulnerability in Trend Micro Apex One and OfficeScan. The vulnerability is due to improper validation of user-supplied file name in the X_DTDAS_Archive_Filename HTTP header when handling a request for sample file upload. Since a remote unauthenticated attacker can control both the file name and file content, this directory traversal vulnerability could allow the attacker to modify executable files in the target system, which could then lead to remote code execution in the context of IUSR account.
Strike Webmin log_parser.pl Stored Cross-Site Scripting	CWE: 74 CVE: 2020-8821	A stored XSS vulnerability exists in Webmin 1.941 and earlier, affecting the Command-Shell module. The flaw is due to lack of HTML character escaping when rendering log entries and is located in 'shell/log_parser.pl' script. An authenticated remote attacker may send a crafted POST body to obtain arbitrary JavaScript execution on a target user's browser.
Strike Cisco HyperFlex HX storfs-asup Handling Remote Command Execution	CWE: 78 CVE: 2021-1498	This strike exploits a remote command execution vulnerability in Cisco HyperFlex. The vulnerability is due to improper sanitization of user supplied data. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could lead to execution of arbitrary code in the context of target process.
Strike SonicWall SMA 100 Appliances Stack-Based Buffer Overflow	CWE: 787 CVE: 2021-20038	This strike exploits stack-based buffer overflow vulnerability in SonicWall SMA 100 Appliances. This vulnerability arises from how environment variables are concatenated into a string within mod_cgi.so and also that the attacker-provided QUERY_STRING is not subjected to any type of length check. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted request to the target server. Successfully exploiting this vulnerability could allow attacker to potentially execute code as a 'nobody' user or crash the affected system.
Strike Zoho ManageEngine ServiceDesk Plus Custom Schedules Command Injection Vulnerability	CVE: 2021-20081	This strike exploits an arbitrary command execution vulnerability in Zoho ManageEngine ServiceDesk Plus. The vulnerability resides in the improper validation of user input within the custom-schedules module. A remote, authenticated attacker could leverage this flaw by sending specially crafted requests, leading to arbitrary command execution and potential remote code execution under the SYSTEM security context.
Strike Arcadyan Buffalo Firmware Path Traversal	CWE: 22 CVE: 2021-20090	This strike exploits a directory traversal vulnerability in Arcadyan Buffalo Firmware. This vulnerability is due to the improper access permission set for a list of folders and files. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation of this vulnerability could lead to read sensitive files, such as configuration files, credentials, or other sensitive information.

Name	References	Description
Strike Zoho ManageEngine ADManager Plus Unrestricted File Upload Vulnerability cve_2021_20130	CVE: 2021-20130	This strike exploits an unrestricted file upload vulnerability in Zoho ManageEngine ADManager Plus. The vulnerability exists due to insufficient validation of uploaded files in the PasswordExpiryAction class. A remote authenticated attacker can leverage this flaw to upload malicious files, potentially leading to remote code execution with SYSTEM privileges.
Strike VMware vCenter vSphere Client Arbitrary File Upload	CWE: 269 CVE: 2021-21972 EXPLOITDB : 49602	This strike exploits a file upload vulnerability in vSphere Client component of VMware vCenter. An remote unauthenticated attacker can send a malicious HTTP POST request to upload an arbitrary file via '/ui/vropspluginui/rest/services/uploadova' api. Successful exploitation may lead to creation and execution of arbitrary files with the context of the NT AUTHORITY\SYSTEM for windows and vsphere-ui user for linux.
Strike VMware View Planner Arbitrary File Upload	CWE: 434 CVE: 2021-21978 EXPLOITDB : 49602	This strike exploits a file upload vulnerability in VMware View Planner. An remote unauthenticated attacker can send a malicious HTTP POST request to upload an arbitrary file via 'logupload' endpoint. Successful exploitation can lead to execution of arbitrary code on the target system with root privileges.
Strike ExifTool DjVu Remote Code Execution	CWE: 74 CVE: 2021-22204	This strike exploits an improper neutralization of directives in dynamically evaluated code ('eval injection') in ExifTool. An remote unauthenticated attacker can supply a malicious crafted DjVu file to be processed via ExifTool. Successful exploitation may lead to execution of arbitrary code with the context of the user running the ExifTool. Note: This strike exploits GitLab CE which runs the ExifTool internally. GitLab also identifies this same vulnerability with CVE-2021-22205.
Strike GitLab Community and Enterprise Edition Remote Command Execution	CWE: 94 CVE: 2021-22205	This strike exploits a remote code execution vulnerability in GitLab Community and Enterprise Editions. This vulnerability is due to improper validation of image files that are passed to file parser. A remote, authenticated attacker could exploit this vulnerability by sending specially crafted image file to an unspecified endpoint. Successfully exploiting this vulnerability could result in remote command execution on the target system.
Strike Advantech iView CommandServlet Directory Traversal Vulnerability	CVE: 2021-22656	This strike exploits a directory traversal vulnerability in Advantech iView. The vulnerability arises from improper validation of user-supplied input in the CommandServlet Java class. A remote, unauthenticated attacker could leverage this flaw by sending crafted HTTP requests, potentially leading to the disclosure of sensitive files and information on the server.
Strike Schneider Electric Struxureware Data Center Expert Command Injection Vulnerability	CVE: 2021-22795	This strike exploits a command injection vulnerability in Schneider Electric Struxureware Data Center Expert. The vulnerability exists due to improper sanitization of the "config" parameter in HTTP POST requests to the "/nbc/compress/repository/test" endpoint. A remote, authenticated attacker could leverage this flaw to execute arbitrary commands on the system with root privileges.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Citrix ShareFile Storage Zones Controller NeatUpload Directory Traversal	CVE: 2021-22941 CWE: 284	The vulnerability allows remote attackers to save files to an arbitrary file path under the web root directory in the NeatUpload library of Citrix ShareFile Storage Zones Controller due to improper validation of an ID parameter in file upload requests. Successful exploitation could result in the execution of arbitrary code on the target server.
Strike Joomla mod_breadcrumbs Title Store Cross-Site Scripting	CWE: 79 CVE: 2021-23124	This strike exploits a cross-site scripting vulnerability in Joomla CMS. This vulnerability is due to inadequate input filtering in the title attribute of mod_breadcrumbs. Successful exploitation could result in arbitrary script code being executed in the security context of the browser.
Strike Oracle Business Intelligence BIRemotingServlet Insecure Deserialization Vulnerability	CVE: 2021-2456	This strike exploits an insecure deserialization vulnerability in Oracle Business Intelligence. The vulnerability arises from improper validation of AMF3 objects in requests to the BIRemotingServlet. A remote attacker can leverage this flaw by sending specially crafted AMF packets, leading to arbitrary code execution in the context of the affected server.
Strike Nagios XI Web SSH Terminal sshterm Cross-Site Scripting	CWE: 79 CVE: 2021-25299	This strike exploits a cross-site scripting vulnerability in Nagios XI 5.7.5 . This vulnerability is due to improper validation of the url parameter in sshterm.php while accessing the web SSH terminal.A remote attacker can exploit this vulnerability by enticing the user to visit a specially crafted link or page. Successful exploitation could result in arbitrary script code being executed in the security context of the browser.
Strike CMS Made Simple Server-Side Template Injection Vulnerability	CVE: 2021-26120	This strike exploits a server-side template injection vulnerability in CMS Made Simple. The vulnerability exists due to improper validation of user-supplied input in the "name" parameter of the "{function}" tag within the Smarty template engine. A remote, authenticated attacker could leverage this flaw to execute arbitrary code on the affected system, potentially gaining full control over the server.
Strike Microsoft Exchange New-DlpPolicy Cmdlet Remote Code Execution Vulnerability	CVE: 2021-26412	This strike targets a remote code execution vulnerability in Microsoft Exchange Server. The issue arises from improper validation of the "commandBlock" tag in DLP policy templates when processing the "ruleParameters" tag. Exploiting this flaw allows an authenticated attacker to execute arbitrary commands with SYSTEM privileges on the affected server.
Strike Microsoft Exchange FilePathName Arbitrary File Write	CVE: 2021-27065 CWE: 73 EXPLOITDB : 49637	An arbitrary file upload vulnerability exist in Microsoft Exchange Server due to lack of sanitization of 'FilePathName' parameter in Virtual Directory reset requests. A remote authenticated attacker may send crafted JSON HTTP requests to upload a webshell on the target system and execute arbitrary commands as the SYSTEM user.

Name	References	Description
Strike Netgear ProSAFE NMS300 Arbitrary File Deletion Vulnerability	CVE: 2021-27272	This strike exploits an arbitrary file deletion vulnerability in Netgear ProSAFE NMS300. The vulnerability resides in the ReportTemplateController class, specifically in the clear() method, which fails to properly sanitize directory traversal characters in the path parameter. A remote authenticated attacker could leverage this flaw by sending crafted HTTP requests to delete arbitrary files on the server, potentially leading to denial-of-service conditions.
Strike Netgear ProSAFE NMS300 Post-Authentication Command Injection Vulnerability	CVE: 2021-27273	This strike exploits a command injection vulnerability in Netgear ProSAFE NMS300. The vulnerability exists due to insufficient validation of the "fileName" parameter in the rebootSystem() method of the SettingConfigController class. A remote, authenticated attacker could leverage this flaw by sending specially crafted HTTP requests, leading to the execution of arbitrary commands with SYSTEM privileges.
Strike Netgear ProSAFE NMS300 Unrestricted File Upload Vulnerability	CVE: 2021-27274	This strike exploits an unrestricted file upload vulnerability in Netgear ProSAFE NMS300. The vulnerability resides in the MFileUploadController class, specifically in the uploadFile() method, which fails to properly validate the file type and parameters of uploaded files. A remote attacker could exploit this vulnerability by uploading a malicious file, leading to arbitrary code execution under the security context of SYSTEM.
Strike Apache Solr ReplicationHandler SSRF Vulnerability	CVE: 2021-27905	This strike exploits a server-side request forgery vulnerability in Apache Solr. The vulnerability is located in the ReplicationHandler's handling of the masterUrl and leaderUrl parameters. Exploiting this vulnerability allows a remote attacker to perform arbitrary file writes, disclose sensitive information, and spoof server conditions.
Strike Apache Superset Markdown Component Stored Cross-Site Scripting	CWE: 79 CVE: 2021-27907	This strike exploits a stored cross-site scripting vulnerability in the Markdown component of Apache Superset. This vulnerability is due to insufficient validation of Markdown snippet in a dashboard. A remote authenticated attacker can exploit this vulnerability by sending crafted requests to the target server. Successful exploitation could result in arbitrary script execution in the target user's browser.
Strike Alibaba Nacos AuthFilter Authentication Bypass Vulnerability	CVE: 2021-29441	This strike exploits an authentication bypass vulnerability in Alibaba Nacos. The vulnerability is located in the AuthFilter servlet filter implementation, specifically in the doFilter method of the AuthFilter class. Exploiting this vulnerability allows a remote, unauthenticated attacker to gain unauthorized access to endpoints that typically require authentication.
Strike Ivanti Avalanche imageFilePath Directory Traversal Vulnerability	CVE: 2021-30497	This strike exploits a directory traversal vulnerability in Ivanti Avalanche. The vulnerability resides in the improper validation of the "imageFilePath" parameter in HTTP requests. A remote, unauthenticated attacker could leverage this flaw to access arbitrary files on the server, potentially leading to the disclosure of sensitive information.
Strike WebSVN Search.php Command Injection Vulnerability	CVE: 2021-32305	This strike exploits a command injection vulnerability in WebSVN. The vulnerability exists due to improper sanitization of the "search" parameter in requests sent to the search.php endpoint. A remote, unauthenticated attacker can leverage this flaw to execute arbitrary commands with the privileges of the web server on the target system.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike SmartStoreNET ForumPost Stored Cross-Site Scripting Vulnerability	CVE: 2021-32608	This strike exploits a stored cross-site scripting vulnerability in SmartStoreNET. The vulnerability resides in the improper handling of BBCode url tags within forum posts. A remote attacker could exploit this flaw by posting maliciously crafted forum messages, leading to arbitrary script execution in the browser of users viewing the affected pages.
Strike Studio-42 elFinder Archive Command Injection Vulnerability	CVE: 2021-32682	This strike exploits a command injection vulnerability in Studio-42 elFinder. The vulnerability resides in the insufficient validation of the "name" parameter when creating an archive in the makeArchive function. A remote, unauthenticated attacker can leverage this flaw to execute arbitrary commands with the privileges of the web server process.
Strike WooCommerce Blocks WordPress Plugin SQL Injection Vulnerability	CVE: 2021-32789	This strike exploits an SQL injection vulnerability in the WooCommerce Blocks WordPress plugin. The vulnerability arises from insufficient input validation in the "calculate_attribute_counts" parameter of the "/wc/store/products/collection-data" API endpoint. A remote, unauthenticated attacker can exploit this flaw by sending crafted HTTP requests, leading to the execution of arbitrary SQL SELECT queries and unauthorized retrieval of database information.
Strike Delta Industrial Automation DIAEnergie Arbitrary File Upload Vulnerability	CVE: 2021-32955	This strike exploits an arbitrary file upload vulnerability in Delta Industrial Automation DIAEnergie. The vulnerability resides in the HandlerPage_KID endpoint due to insufficient input validation on the HtmlId parameter and lack of authentication. A remote, unauthenticated attacker could leverage this flaw to upload malicious files, potentially leading to arbitrary code execution on the server.
Strike Foxit Reader and Editor Use-After-Free Vulnerability in Annotation Handling	CVE: 2021-34833	This strike exploits a use-after-free vulnerability in Foxit PDF Reader and Editor. The vulnerability resides in the improper handling of the author property of Annotation objects within JavaScript. Exploiting this flaw allows a remote attacker to execute arbitrary code by enticing a user to open a maliciously crafted PDF file.
Strike Hikvision Improper Input Validation	CWE: 78 CVE: 2021-36260	This strike exploits a command injection vulnerability in Hikvision IP camera/NVR firmware. The vulnerability is due to the insufficient input validation. It inserts a command into an XML payload used with an HTTP PUT request sent to the '/SDK/webLanguage' endpoint, resulting in command execution as the root user. A remote, unauthenticated attacker could exploit the vulnerability to launch a command injection attack by sending some messages with malicious commands.
Strike Nagios XI Post-auth RCE through Path Traversal	CWE: 22 CVE: 2021-37343	This strike exploits a path traversal vulnerability in Nagios XI versions prior to 5.8.5 . This vulnerability is due to improper validation of the job parameter in autodiscovery feature. A remote authenticated attacker can exploit this vulnerability by sending a crafted request. Successful exploitation could result in arbitrary file creation and further more can result in arbitrary code being executed in the context of the web server. Note: This strike contains just the authentication and the request required to create a backdoor in the web server.

Name	References	Description
Strike Centreon ProceduresProxy.class.php SQL Injection Vulnerability	CVE: 2021-37558	This strike exploits an SQL injection vulnerability in the Centreon web application. The vulnerability is located in the ProceduresProxy.class.php file, specifically within the getHostId() and getServiceId() functions, which fail to properly sanitize the host_name and service_description parameters. Exploiting this vulnerability allows a remote, unauthenticated attacker to execute arbitrary SQL commands on the database, potentially leading to unauthorized data manipulation or further compromise of the target system.
Strike Zoho ManageEngine ADManager Plus Unrestricted File Upload Vulnerability cve_2021_37921	CVE: 2021-37921	This strike targets an unrestricted file upload vulnerability in Zoho ManageEngine ADManager Plus. The issue arises from insufficient validation of uploaded files in the ReportsAction class. Exploiting this flaw allows a remote authenticated attacker to upload arbitrary files, potentially leading to remote code execution with SYSTEM privileges.
Strike Zoho ManageEngine ADManager Plus Unrestricted File Upload Vulnerability cve_2021_37926	CVE: 2021-37926	This strike exploits an unrestricted file upload vulnerability in Zoho ManageEngine ADManager Plus. The vulnerability exists due to insufficient validation of file types in the LicenseAction class when handling uploaded files. A remote authenticated attacker can leverage this flaw to upload malicious files, potentially leading to remote code execution with SYSTEM-level privileges.
Strike Google Chrome Hole Memory Corruption	CWE: 755 CVE: 2021-38003	This strike exploits a vulnerability in the V8 in Google Chrome. The vulnerability exists due to improper handling of the internal TheHole value when an exception occurs during execution. By crafting specific inputs, it is possible to trigger a scenario where TheHole leaks into JavaScript code. Successful exploitation could result in memory corruption.
Strike Microsoft Azure Open Management Infrastructure Authentication Bypass	CWE: 305 CVE: 2021-38647	This strike exploits an authentication bypass vulnerability in Microsoft Azure Open Management Infrastructure. The vulnerability is due to improper validation of the Authorization header in the HTTP request supplied. A remote attacker could exploit this vulnerability by sending a crafted request to a vulnerable server. A successful attack might result in the remote code execution in the context of root user.
Strike VMware NSX Manager XStream Remote Code Execution Vulnerability	CWE: 502 CVE: 2021-39144	This strike exploits an insecure deserialization vulnerability in the XStream library in VMWare NSX Manager. This flaw, originally identified as an XStream deserialization issue, leverages the application's XML processing to execute arbitrary code. Due to inadequate input validation in XStream, the application deserializes untrusted XML data insecurely. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted XML payload to an unauthenticated API endpoint. Successful exploitation could allow the attacker to execute code with elevated privileges, potentially leading to full system compromise.
Strike Nagios XI Custom Includes Component Arbitrary File Upload Vulnerability	CVE: 2021-40344	This strike exploits an arbitrary file upload vulnerability in the Custom Includes component of Nagios XI. The vulnerability resides in the misconfiguration of the .htaccess file within the /images subdirectory of the component. A remote, authenticated attacker can leverage this flaw to upload and execute malicious PHP code, potentially leading to arbitrary code execution under the web server's security context.

Name	References	Description
Strike Nagios XI cmdsubsys.php Command Injection Vulnerability	CVE: 2021-40345	This strike targets a command injection vulnerability in the cmdsubsys.php script of Nagios XI. The issue arises from improper sanitization of user-supplied input in the names of files within uploaded Zip archives. Exploiting this flaw allows a remote, authenticated attacker to execute arbitrary commands with the privileges of the nagios user.
Strike Aviatrix Controller Unrestricted File Upload	CVE: 2021-40870 CWE: 23	This strike exploits a file upload vulnerability in Aviatrix Controller. The vulnerability allows unauthenticated attackers to upload malicious files, which can then be exploited via directory traversal to execute arbitrary code. Successful exploitation of this vulnerability allows remote attackers to execute arbitrary commands on the affected system.
Strike Netgate pfSense diag_routes.php Command Injection Vulnerability	CVE: 2021-41282	This strike exploits a command injection vulnerability in Netgate pfSense. The vulnerability resides in the diag_routes.php file due to insufficient validation of user-supplied input in the filter parameter. A remote, authenticated attacker can leverage this flaw to execute arbitrary operating system commands, potentially leading to full system compromise.
Strike Ivanti Avalanche Central FileStore Command Injection Vulnerability	CVE: 2021-42129	This strike exploits a command injection vulnerability in Ivanti Avalanche Enterprise Service. The vulnerability exists due to insufficient validation of input fields in the Central FileStore configuration settings. A remote, authenticated attacker could leverage this flaw by sending crafted requests, leading to the execution of arbitrary commands on the server with SYSTEM privileges.
Strike Zoho ManageEngine Network Configuration Manager Ping Command Injection	CWE: 77 CVE: 2021-43319	This strike exploits a command injection vulnerability in Zoho ManageEngine Network Configuration Manager. The vulnerability is due to insufficient validation in the ipaddress field of the ping functionality in add device web interface. A remote, authenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could lead to arbitrary code execution in the security context of the web server. *Note : Upon running the strike in one-arm mode a file named Test is created in /tmp directory of the vulnerable server. The default credentials being used are admin/admin.
Strike FusionPBX fax_send.php Command Injection Vulnerability	CVE: 2021-43405	This strike exploits a command injection vulnerability in the fax_send.php script of FusionPBX. The vulnerability exists due to insufficient input validation of the fax_extension parameter in HTTP requests. Exploiting this flaw allows a remote, authenticated attacker to execute arbitrary system commands with the privileges of the server process.
Strike Roundcube Webmail SQL Injection Vulnerability	CWE: 89 CVE: 2021-44026	This strike exploits an SQL injection vulnerability in Roundcube. The vulnerability is due to insufficient validation of user-provided search_params data. To execute the attack, the malicious actor must first authenticate within a Roundcube session. Upon successful exploitation, the attacker could read sensitive information, modify database content, or escalate privileges based on the permissions granted to the database account that Roundcube utilizes.

Name	References	Description
Strike Zoho ManageEngine ImportTechniciansAction Arbitrary File Upload	CWE: 287 CVE: 2021-44077	This strike exploits an arbitrary file write vulnerability that has been reported in Zoho ManageEngine ServiceDesk Plus, ServiceDesk Plus MSP, and SupportCenter Plus. The vulnerability is due to insufficient validation of input data. An unauthenticated remote attacker can exploit this vulnerability by submitting a crafted request to the target server. Successful exploitation results in the writing of an arbitrary file to the target application, potentially leading to execution of arbitrary code as SYSTEM.
Strike Zoho Desktop Central Authentication Bypass Vulnerability	CWE: 287 CVE: 2021-44515	This strike exploits an authentication bypass vulnerability in ManageEngine Desktop Central. The vulnerability is due to an input validation error in the StateFilter class. A remote, unauthenticated attacker could bypass the authentication of the console component and then send commands via WebSockets to the managed devices by the ManageEngine Desktop Central server. This may potentially cause remote code execution, allowing a malicious, unauthenticated attacker to execute arbitrary code on the devices managed by the ManageEngine Desktop Central server.
Strike Ivanti EPM Cloud Services Appliance Code Injection Vulnerability	CWE: 94 CVE: 2021-44529	This strike exploits a command injection vulnerability in the Ivanti Cloud Services Appliance (CSA) for Ivanti Endpoint Manager. The vulnerability is due to insufficient input validation and improper handling of cookie data. The vulnerable code allows an unauthenticated attacker to inject and execute arbitrary PHP code by crafting specific cookie headers, leading to execution of base64-encoded payloads via the eval() function. Successful exploitation results in command execution as the 'nobody' user.
Strike Apache httpd mod_lua Integer Underflow	CWE: 191 CVE: 2021-44790	A integer underflow vulnerability exists in multiple versions of Apache Software Foundation httpd prior to 2.4.52. The flaw is due to improper handling of the request body. An unauthenticated remote attacker may sent a crafted request to the target server. Successful exploitation could result in remote code execution or denial of service condition. * Target Apache server must have the mod_lua module enabled and have the lua-script handler set for Lua scripts stored on the server. * The target must contain a Lua script utilizing the r:parsebody() function.
Strike D Link Multiple Routers Remote Code Execution Vulnerability	CVE: 2021-45382 CWE: 78	This strike exploits an OS command injection vulnerability in D-Link Routers. The vulnerability is due to insufficient validation of user supplied input. An unauthenticated attacker could exploit this vulnerability by sending a crafted HTTP request and might result in remote code execution.
Strike WordPress Photo Gallery Plugin SQL Injection Vulnerability	CVE: 2022-0169	This strike exploits a SQL injection vulnerability in the WordPress Photo Gallery plugin. The vulnerability arises from improper sanitization of the `bwg_tag_id_bwg_thumbnails_0` parameter in HTTP requests. A remote, unauthenticated attacker can leverage this flaw to execute arbitrary SQL commands on the database, potentially leading to data exfiltration or unauthorized access.

Name	References	Description
Strike Oracle JDeveloper ADF Faces Deserialization of Untrusted Data Vulnerability	CVE: 2022-21445 CWE: 502	This strike exploits an insecure deserialization vulnerability in Oracle JDeveloper ADF Faces. The vulnerability is due to insufficient validation of HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending crafted HTTP request to the vulnerable server. Successful exploitation of this vulnerability could lead to remote code execution in the context of the user using the vulnerable server.
Strike Apache httpd mod_lua req_parsebody Denial of Service	CWE: 665 CVE: 2022-22719	This strike exploits a denial of service vulnerability in Apache httpd. The vulnerability is due to use of uninitialized memory when processing a request. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could lead to crash of the server and with extended exploitation may lead to denial of service conditions.
Strike SalesAgility SuiteCRM email_recipients Remote Code Execution Vulnerability	CVE: 2022-23940	This strike exploits a remote code execution vulnerability in SalesAgility SuiteCRM. The vulnerability is located in the improper input validation of the "email_recipients" parameter within HTTP POST requests. Exploiting this vulnerability allows a remote, authenticated attacker to execute arbitrary code on the target server.
Strike Apache APISIX batch-requests Plugin IP address Restriction Bypass	CWE: 290 CVE: 2022-24112	This strike exploits an authentication weakness vulnerability in Apache APISIX. The vulnerability is due to inefficient validation of client requests at the vulnerable API endpoint "/apisix/admin/batch-requests". A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the vulnerable server if the batch-requests plugin is enabled and it is using the default API key of the administrator. Successful exploitation could lead to arbitrary code execution under the security context of the server process. *NOTE: While running this strike in OneArm mode, it creates a new endpoint/route "/poc/testing" which is visited to execute a command to create a file called "poc" under the "/tmp" directory on the server.
Strike MyBB Admin Control Panel Code Injection Vulnerability	CVE: 2022-24734	This strike targets a code injection vulnerability in the MyBB Admin Control Panel. The issue arises from improper input validation when processing user-supplied data in the settings management functionality. Exploiting this vulnerability allows a remote, authenticated attacker to execute arbitrary PHP code on the server with the privileges of the web application.
Strike TerraMaster TOS Unauthenticated Remote Code Execution	CWE: 74 CVE: 2022-24989	This strike exploits an unauthenticated command injection vulnerability in TerraMaster TOS. The vulnerability is due to the improper sanitization of the user input used in the popen function of the createRaid function. The vulnerability when chained with CVE-2022-24990 allows a remote unauthenticated attacker to execute arbitrary code as root through the raidtype and diskstring parameters during PHP Object Instantiation at the api.php?mobile/createRaid endpoint. Successful exploitation could result in arbitrary code execution under the security context of the user running the vulnerable application with root privileges.

Name	References	Description
Strike TerraMaster TOS Sensitive Information Leak Vulnerability	CWE: 306 CVE: 2022-24990	This strike exploits a sensitive information leak vulnerability in TerraMaster TOS. The vulnerability arises due to webNasIPS function in TerraMaster NAS devices which skips authentication checks. Attackers can exploit this vulnerability to obtain sensitive information like the admin password hash without authentication. The vulnerability when chained with CVE-2022-24989 allows a remote unauthenticated attacker to execute arbitrary code as root. Successful exploitation could result in information disclosure and in the worst case it could lead to remote code execution under the security context of the target server.
Strike Delta Industrial Automation DIAEnergie Arbitrary File Upload Vulnerability cve_2022_25347	CVE: 2022-25347	This strike exploits an arbitrary file upload vulnerability in Delta Industrial Automation DIAEnergie. The vulnerability resides in the HandlerPage_KID endpoint, where insufficient input validation is performed on the HtmlId parameter and file extensions during file upload processing. A remote, unauthenticated attacker could leverage this flaw to upload malicious files to arbitrary locations on the server, potentially leading to the execution of arbitrary code within the web server's context.
Strike Open-Falcon Falcon-Plus SQL Injection in GetHostsFromGroup Function	CVE: 2022-26245	This strike exploits a SQL injection vulnerability in Open-Falcon Falcon-Plus. The vulnerability exists due to improper sanitization of user input in the /proc/group API endpoint. A remote attacker could leverage this flaw by sending a specially crafted request, leading to arbitrary SQL query execution on the database.
Strike dotCMS processFile Directory Traversal	CWE: 22 CVE: 2022-26352	This strike exploits a Directory Traversal vulnerability in dotCMS. The vulnerability is due to insufficient validation of the names of files uploaded through the dotCMS content API. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in writing a file outside of the expected document root, possibly leading to, in the worst case, arbitrary code execution under the security context of the web server process. *NOTE: While running this strike in OneArm mode, a file named "poc.jsp" is created on the server.
Strike Delta Industrial Automation DIAEnergie SQL Injection Vulnerability in DIAE_loopmapHandler.ashx	CVE: 2022-26887	This strike exploits an SQL injection vulnerability in Delta Industrial Automation DIAEnergie. The vulnerability resides in the insufficient input validation of the "kid" parameter in HTTP requests to the DIAE_loopmapHandler.ashx endpoint. A remote, unauthenticated attacker could exploit this vulnerability by sending specially crafted requests, leading to the execution of arbitrary SQL commands with the privileges of NT SERVICE\MSSQLSERVER.
Strike Studio-42 elFinder Unrestricted File Upload Vulnerability	CVE: 2022-27115	This strike exploits an unrestricted file upload vulnerability in Studio-42 elFinder. The vulnerability resides in the improper validation of filenames during file uploads via the connector.minimal.php endpoint on Windows systems. Exploiting this vulnerability allows a remote, unauthenticated attacker to upload files with restricted extensions or malicious content, potentially leading to remote code execution.

Name	References	Description
Strike QNAP Photo Station Externally Controlled Reference Vulnerability	CWE: 610 CVE: 2022-27593	This strike exploits an externally controlled reference to a resource vulnerability in QNAP NAS devices running Photo Station. The vulnerability arises from an anomaly in PHP's fopen function, enabling an attacker to manipulate the 'g' parameter to traverse outside the intended cache directory and write cached files to arbitrary locations. Successful exploitation of this vulnerability would enable an attacker to modify system files. A remote, unauthenticated attacker could potentially fill up storage areas or exhaust other critical resources on the NAS, leading to denial of service for legitimate users or services dependent on those resources.
Strike Zoho ManageEngine OpManager SQL Injection in Inventory Reports	CVE: 2022-27908	This strike exploits a SQL injection vulnerability in Zoho ManageEngine OpManager. The vulnerability resides in the Inventory Reports module due to insufficient validation of HTTP request parameters. A remote, authenticated attacker could leverage this flaw to execute arbitrary SQL queries, potentially compromising the underlying database.
Strike Zimbra Collaboration MailboxImportServlet Authenticated Directory Traversal	CWE: 22 CVE: 2022-27925	This strike exploits an authenticated directory traversal vulnerability in Zimbra Collaboration. The vulnerability is due to improper validation of zip files uploaded to the MailboxImportServlet. A remote, authenticated attacker could exploit this vulnerability by uploading a crafted zip file to the target server. Successful exploitation could result in the attacker writing files outside of the expected document root, in the worst case, leading to arbitrary code execution under the security context of the server process.
Strike SolarView Compact Command Injection	CWE: 78 CVE: 2022-29303	This strike exploits a command injection vulnerability in SolarView Compact. This vulnerability lies in the conf_mail.php component of the SolarView application. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted post request to the target server. Successful exploitation of this vulnerability could lead to remote code execution.
Strike WSO2 API Manager Directory Traversal	CWE: 434 CVE: 2022-29464	This strike exploits a directory traversal vulnerability in WSO2 API Manager. The vulnerability is due to improper sanitization for the multipart form field name for the file upload route. A remote, unauthenticated attacker could exploit the vulnerability by sending crafted HTTP requests to a target server. Successful exploitation can result in arbitrary file write in the context of the wso2carbon user.
Strike Lansweeper HelpdeskActions.aspx Directory Traversal Vulnerability	CVE: 2022-29517	This strike exploits a directory traversal vulnerability in Lansweeper. The vulnerability exists due to insufficient sanitization of the inline attachment file names when editing templates. A remote, authenticated attacker could leverage this flaw to write arbitrary files to the target system, potentially leading to denial of service or other malicious outcomes.
Strike WWBN AVideo unzipDirectory Directory Traversal Vulnerability	CVE: 2022-30547	This strike exploits a directory traversal vulnerability in WWBN AVideo. The vulnerability resides in the unzipDirectory function within the objects/functions.php file, which fails to properly sanitize file names during ZIP file extraction. A remote, authenticated attacker could leverage this flaw by uploading a crafted ZIP file, enabling arbitrary file writes and potential code execution within the web server's security context.

Name	References	Description
Strike Lansweeper AssetActions.aspx Directory Traversal Vulnerability	CVE: 2022-32573	This strike exploits a directory traversal vulnerability in Lansweeper. The vulnerability exists due to improper sanitization of the "txtdocname" parameter when processing file uploads. Exploiting this flaw allows a remote, authenticated attacker to perform arbitrary file writes on the target system, potentially leading to denial of service or other malicious outcomes.
Strike ZK Framework Authentication Bypass	CWE: 200 CVE: 2022-36537	This strike exploits an authentication bypass vulnerability in ZK Java Framework. The vulnerability is due to lack of authentication in ZK AuUploader servlet. A remote unauthenticated attacker can exploit this vulnerability sending a crafted request to the victim server which leads to the disclosure of sensitive files in the context of the webroot.
Strike Zimbra Collaboration MailboxImportServlet Authentication Bypass	CWE: 22 CVE: 2022-37042	This strike exploits an authentication bypass vulnerability in Zimbra Collaboration. The vulnerability is due to improper validation of zip files uploaded to the MailboxImportServlet. A remote, unauthenticated attacker could exploit this vulnerability by uploading a crafted zip file to the target server. Successful exploitation could result in the attacker writing files outside of the expected document root, in the worst case, leading to arbitrary code execution under the security context of the server process.
Strike Adobe ColdFusion Directory Traversal and Arbitrary Code Execution Vulnerability	CVE: 2022-38421	This strike exploits a directory traversal vulnerability in Adobe ColdFusion. The vulnerability exists due to improper input validation when processing HTTP parameters in the copydirectory.cfm script. A remote, authenticated attacker could leverage this flaw to execute arbitrary code with SYSTEM privileges on the target server.
Strike Apache Airflow DAG run_id Command Injection	CWE: 94 CVE: 2022-40127	This strike exploits a command injection vulnerability in Apache Airflow. This vulnerability is due to improper input validation for parameter run_id for directed acyclic graphs or DAGs. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successfully exploiting this vulnerability could result in command execution in the context of the user running the server. *NOTE : In one-arm mode, the strike uses airflow/ airflow to login and uses example_bash_operator DAG for exploitation which results in /tmp/Test file being created.
Strike Dolibarr ERP and CRM Code Injection Vulnerability in edit.php	CVE: 2022-40871	This strike exploits a code injection vulnerability in Dolibarr ERP and CRM. The vulnerability resides in the insufficient sanitization of parameters in HTTP POST requests to the edit.php endpoint. Successful exploitation allows a remote attacker to execute arbitrary PHP code on the target server, potentially leading to remote code execution.
Strike Microsoft Exchange Server Server-Side Request Forgery Vulnerability	CWE: 918 CVE: 2022-41040	This strike exploits a server-side request forgery vulnerability in Microsoft Exchange Server. The vulnerability is due to insufficient handling of requests to the autodiscover component of Exchange. An authenticated, remote attacker can exploit this vulnerability by sending a crafted request to the vulnerable Exchange server. Successful exploitation results in requests being made to backend servers. *NOTE: This strike sends a request to /mapi/nsipi/ or ews/exchange.asmx which are inaccessible by default. In one-arm mode we use the authorization Administrator:Password1

Name	References	Description
Strike Centreon Web Poller Resource SQL Injection Vulnerability	CVE: 2022-41142	This strike exploits a SQL injection vulnerability in the Centreon Web Poller Resource module. The vulnerability exists due to insufficient input validation of the `resource_activate[resource_activate]` parameter in the `insertResource` function. A remote, authenticated attacker could leverage this flaw by sending a specially crafted HTTP request, potentially leading to arbitrary SQL command execution on the target database.
Strike Centreon Web formContactGroup.php SQL Injection Vulnerability	CVE: 2022-42427	This strike exploits an SQL injection vulnerability in the Centreon Web application. The vulnerability exists due to improper validation of the `cg_id` parameter in the `formContactGroup.php` script. A remote, authenticated attacker could leverage this flaw by sending a specially crafted HTTP request, potentially leading to the execution of arbitrary SQL commands on the database.
Strike Zoho ManageEngine Password Manager Pro UserGroupListTable Controller SQL Injection	CWE: 89 CVE: 2022-43672	The strike exploits an SQL injection vulnerability in Zoho ManageEngine Password Manager Pro and related products. The vulnerability is due to improper validation of actionType parameter in the UserGroupListTableController class. A remote attacker can exploit the vulnerability by sending a crafted request to the target server. Successful exploitation could lead to arbitrary SQL code execution in the security context of database service, which runs as SYSTEM.
Strike Atlassian Bitbucket Server and Data Center Command Injection Vulnerability	CWE: 77 CVE: 2022-43781	This strike exploits a command injection vulnerability in Atlassian Bitbucket Server and Data Center. The vulnerability is due to improper validation of usernames on the server. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in arbitrary command execution in the security context of the user running the vulnerable application. *NOTE: While running this strike in OneArm mode, a file /tmp/poc is created on the server.
Strike TP-Link Archer AX21 Country Command Injection	CVE: 2023-1389 CWE: 77	This strike exploits a command injection vulnerability in TP-Link Archer AX21. The vulnerability is due to the improper sanitization of the country parameter. A remote, unauthenticated attacker could exploit this vulnerability by injecting the commands into the country parameter. Execution requires sending the request twice, the first request sets the command in the country value, and the second request executes it. Successful exploitation could allow an attacker to achieve remote code execution with root privileges.
Strike Sophos Web Appliance Command Injection Vulnerability	CWE: 77 CVE: 2023-1671	This strike exploits a pre-auth command injection vulnerability in the warn-proceed handler of the Sophos Web Appliance. The vulnerability arises due to improper sanitization of user-provided input. It allows a remote, unauthenticated attacker to inject commands through the data field by escaping commands with a single quote. Successful exploitation could result in arbitrary code execution under the security context of the user running the vulnerable application.

Name	References	Description
Strike WordPress Limit Login Attempts Plugin Stored Cross Site Scripting	CWE: 79 CVE: 2023-1861	A stored cross-site scripting vulnerability has been discovered in WordPress Limit Login Attempts Plugin. The vulnerability is due to improper input validation of the cookie value. A remote, unauthenticated attacker could exploit this vulnerability by sending requests with crafted cookie to the target system. Successful exploitation could result in stored cross-site scripting. The vendor has released a patch to address this vulnerability in plugin version 1.7.2.
Strike Cisco IOS XE WebUI Authentication Bypass	CWE: 284 CVE: 2023-20198	This strike exploits an authentication bypass vulnerability in the WebUI component of Cisco IOS XE. This vulnerability is due to improper configuration of the nginx reverse proxy server. A remote, unauthenticated attacker can exploit this vulnerability to bypass authentication by accessing an internal endpoint. Successful exploitation results in the ability to issue privilege commands, including to create a new local user.
Strike Cisco IOS XE WebUI Command Injection	CWE: 78 CVE: 2023-20273	This strike exploits a command injection vulnerability in the WebUI component of Cisco IOS XE. This vulnerability is due to insufficient validation of IPv6 addresses supplied when performing a software upgrade. A remote, authenticated attacker can exploit this vulnerability by sending crafted HTTP requests to the target server. Successful exploitation results in the execution of arbitrary OS commands with the privileges of root.
Strike Vmware Aria Operations for Networks resttosaasservlet Command Injection Vulnerability	CWE: 77 CVE: 2023-20887	This strike exploits a command injection vulnerability in Vmware Aria Operations for Networks. The vulnerability is due to improper input handling in API requests and an Nginx misconfiguration that allows access to the restricted internal API endpoint /resttosaasservlet. A remote, unauthenticated attacker can exploit this vulnerability by sending specially crafted requests, bypassing the Nginx reverse proxy configuration. Successful exploitation can lead to the execution of arbitrary commands on the underlying operating system with root privileges, potentially resulting in full system compromise.
Strike VMWare Aria Operations for Networks saveFileToDisk Directory Traversal Vulnerability	CWE: 22 CVE: 2023-20890	This strike exploits a directory traversal vulnerability in VMWare Aria Operations for Networks. The vulnerability is due to improper validation of file names when uploading files to the appliance. The filename parameter from the multipart request is not sanitized before it is used to create a path to the file. A remote, authenticated attacker could exploit this vulnerability by sending crafted requests to the target server. Successful exploitation will allow an attacker to write files outside of the expected temp directories. In the worst case, this could be leveraged to achieve arbitrary code execution under the security context of the root user.

Name	References	Description
Strike Wordpress WpForo Plugin LFI SSRF Deserialization	CWE: 98 CVE: 2023-2249	This strike exploits a File Inclusion and Server Side Request Forgery (SSRF) vulnerability in wpforo plugin of wordpress. This vulnerability is due to lack of input validation for the image_blob parameter which is passed to the php get_file_contents method call. A remote, authenticated low-privileged attacker could exploit this vulnerability by sending a crafted request to the target wordpress server. A successful attack may result in local file inclusion, server side request forgery or insecure deserialization in the server. *NOTE: In one-arm, the strike attempts to login with the creds - 'victimtest/1234' and attempts to fetch the contents of /etc/passwd or reach an internal endpoint at 'http://10.39.44.149:4445/secret' depending on the variant being ran.
Strike Atlassian Confluence Data Center and Server Setup Action Privilege Escalation	CWE: 863 CVE: 2023-22515	This strike exploits a privilege escalation vulnerability in Atlassian Confluence Data Center and Server. The vulnerability is attributed to a weakness in access control within the setup actions component. Its root cause lies in the attacker's ability to execute complex getter/setter chains on the Action object for unauthenticated endpoints, allowing manipulation of crucial properties. Through the modification of the setupComplete variable, the attacker successfully exploited the setup functionality, resulting in the creation of a new administrator user. An unauthenticated, remote attacker could leverage this vulnerability by sending meticulously crafted requests to the setup endpoint. Successful exploitation could lead to the execution of arbitrary code within the security context of the newly created administrator user.
Strike Atlassian Confluence Data Center and Server Improper Authorization	CWE: 863 CVE: 2023-22518	This strike exploits an improper authorization vulnerability in Atlassian Confluence Data Center and Server. The vulnerability arises from the absence of authentication for legacy endpoints associated with the application restore feature, specifically the "/json/setup-restore.action" endpoint. Given the lack of authentication requirements for accessing this endpoint, a malicious actor could exploit this vulnerability to delete all data in a Confluence installation and replace it with data under their control. A remote, unauthenticated attacker could leverage this vulnerability by sending carefully crafted requests to the target server. If successfully exploited, this could lead to privilege escalation and the potential execution of arbitrary code on the targeted system.
Strike Atlassian Confluence Data Center and Server Template Injection	CWE: 74 CVE: 2023-22527	This strike exploits a template injection vulnerability in Atlassian Confluence Data Center and Server. The vulnerability is due to improper validation of user data sent to the sever. The label parameter is not properly escaped before use in an OGNL expression. This allows arbitrary OGNL expression evaluation. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted requests to the target server. Successful exploitation could result in arbitrary code execution under the security context of the user running the vulnerable application. *NOTE: While running the strike in one-arm mode, a file gets created in the /tmp directory of the vulnerable server.

Name	References	Description
Strike Zoho ManageEngine SupportCenter Plus Command Injection via Custom Schedules Executor	CVE: 2023-23076	This strike exploits a command injection vulnerability in Zoho ManageEngine SupportCenter Plus. The vulnerability exists due to insufficient validation of the "executor" parameter in the custom schedule settings. A remote, authenticated attacker could leverage this flaw by sending specially crafted requests, leading to arbitrary command execution with SYSTEM privileges.
Strike Joomla CMS Webservice Authentication Bypass	CWE: 284 CVE: 2023-23752	This strike exploits an authentication bypass vulnerability in Joomla CMS. The vulnerability is due to inadequate sanitization of request parameters when processing API requests. If the request includes a 'public' parameter its value will overwrite the route default variable, and unauthenticated access may be granted to private API routes. An unauthenticated remote attacker can manipulate request parameters, leading to potential unauthorized access to private API routes that require authentication. Successful exploitation could result in sensitive information disclosure, including Joomla database credentials. Attackers could leverage this information to gain unauthorized access, modify user passwords, or perform brute-force attacks on user accounts. *Note: Running this strike in one-arm mode reveals the database credentials and other sensitive information.
Strike D-Link DIR-820 Router ping ccp OS Command Injection	CVE: 2023-25280 CWE: 78	This strike exploits an OS command injection vulnerability in D-Link DIR-820 Router. The vulnerability is due to improper sanitization of ping_addr parameter used in ping ccp endpoint. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted payload to the ping_addr parameter. Successful exploitation could result in remote code execution on the affected device and potential escalation of privileges to root.
Strike Ruckus Wireless Admin Unauthenticated RCE	CWE: 94 CVE: 2023-25717	This strike exploits a remote code execution vulnerability in Ruckus Wireless routers. The vulnerability is due to insufficient input validation in the '/forms/doLogin' endpoint of the admin web page. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the victim router which results in remote code execution.
Strike PaperCut MF and NG SetupCompleted formSubmit Authentication Bypass	CVE: 2023-27350 CWE: 284	This strike exploits an authentication bypass vulnerability in PaperCut MF/NG. The vulnerability is due to improper access and authentication control in "SetupCompleted" class. A remote, unauthenticated attacker could exploit the vulnerability by sending a request to the "/app" endpoint on the target server. Successful exploitation could result in authentication bypass and, in the worst case, arbitrary code execution on the server under the security context of SYSTEM. *NOTE - While running this strike in OneArm mode, windows calculator application runs on the target server.
Strike Zoho ManageEngine ADSelfService Plus Mobile App Authentication API Denial of Service	CWE: 476 CVE: 2023-28342	This strike exploits an authentication bypass vulnerability in Zoho ManageEngine ADSelfService Plus. The vulnerability is due to improper input validation in the Mobile App Authentication API. A remote, unauthenticated attacker could send a crafted request to the authentication endpoint without a password parameter. When the target server processes the request, it will pass the null password value to a native function resulting in an access violation and subsequently terminating and restarting the server process. Successfull exploitation could result in denial of service.

Name	References	Description
Strike Contec CONPROSYS HMI System SQL Injection Vulnerability	CVE: 2023-29154 CWE: 89	This strike exploits an SQL injection vulnerability in Contec CONPROSYS HMI System. The vulnerability is due to insufficient sanitization of user data used in query_getTableCol.php. The query retrieves the metadata of the database table. However, the code fails to check for SQL injection characters in the JSON parameter of the table. As a result, a remote, authenticated attacker could exploit this vulnerability by sending a specially crafted request to the target server. A successful attack may allow the execution of arbitrary SQL commands against the database on the target server.
Strike Ghost CMS static-theme.js Directory Traversal Vulnerability	CVE: 2023-32235	This strike exploits a directory traversal vulnerability in Ghost CMS. The vulnerability resides in the static-theme.js component, where user-supplied paths are improperly validated. A remote attacker could leverage this flaw to access sensitive files on the server, potentially exposing confidential information.
Strike Ignite Realtime Openfire Path Traversal Vulnerability	CWE: 22 CVE: 2023-32315	This strike exploits a path traversal vulnerability in Ignite Realtime Openfire. This vulnerability is due to the improper handling of UTF-16 encoded characters in URLs. It allows an unauthenticated user to use an already configured Openfire environment to access restricted pages in the Admin Console reserved for administrative users. This vulnerability can be used to create a new admin user, which can then be used to upload a Openfire management plugin weaponized with a Java native payload that triggers an RCE. Successful exploitation could result in authentication bypass and remote code execution through access to the restricted Admin Console pages. *NOTE: While running the strike in one-arm mode, the CSRF token can be retrieved from the response, which can be further used to create a new admin user account.
Strike Jenkins Sidebar Link Plugin icon Directory Traversal Vulnerability	CVE: 2023-32985 CWE: 22	This strike exploits a directory traversal vulnerability in Jenkins Sidebar Link Plugin. This vulnerability is due to a directory traversal when handling link icons. The vulnerability exists when the function SidebarLinkPlugin.doCheckLinkIcon() is called, the value of the parameter value or the path that is created is never sanitized or normalized of directory traversal related characters. A remote, authenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successfully exploiting this vulnerability could result in information disclosure. *NOTE: While running this strike in OneArm mode, the existence of the file "/etc/passwd" on the target server is checked. The credentials used are as follows: the username is "jenkins_user" and the password is "jenkins".
Strike Zimbra Webmail Draftid Cross-Site Scripting	CWE: 79 CVE: 2023-34192	This strike exploits a cross-site scripting vulnerability in the web component of Zimbra Collaboration Suite. The vulnerability is due to improper input sanitization. A remote authenticated attacker could exploit this vulnerability by sending a crafted request to the target system. Successful exploitation could result in execution of script code in the security context of the target user's browser.

Name	References	Description
Strike Google Chrome V8 Engine JSStackCheck Type Confusion	CWE: 843 CVE: 2023-3420	This strike exploits a type confusion vulnerability in the V8 JavaScript engine of Google Chrome. The vulnerability is due to incorrect side effect modelling of JSStackCheck. A remote attacker could exploit this vulnerability by enticing a user into opening a crafted HTML page. Successful exploitation could result in execution of arbitrary code in the context of the Google Chrome sandbox.
Strike Ivanti Endpoint Manager Mobile (EPMM) and MobileIron Core Authentication Bypass	CWE: 287 CVE: 2023-35082	This strike exploits an authentication bypass vulnerability in Ivanti Endpoint Manager Mobile. The vulnerability is due to a logic flaw and allows a remote unauthenticated attacker to access API endpoints on exposed management servers or resources without proper authentication. This access grants them the ability to execute various operations, potentially compromising sensitive information or modifying platform configurations.
Strike Ivanti MobileIron Sentry uploadFileUsingFile Input Authentication Bypass Vulnerability	CWE: 863 CVE: 2023-38035	This strike exploits an authentication bypass vulnerability in MICS Admin Portal in Ivanti MobileIron Sentry. A remote, unauthenticated attacker can bypass authentication controls on the administrative interface due to an insufficiently restrictive Apache HTTPD configuration. Successful exploitation of this vulnerability could allow an attacker to bypass authentication and gain unauthorized access to the system.
Strike Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	CWE: 502 CVE: 2023-38203	This strike exploits an insecure deserialization vulnerability in Adobe ColdFusion. The vulnerability is due to inadequate filtering of Java class paths during the deserialization process, allowing remote, unauthenticated attackers to send maliciously crafted serialized objects. These objects can lead to arbitrary code execution within the application. ColdFusion uses a denylist to prevent certain classes from being deserialized, however, the class com.sun.rowset.JdbcRowSetImpl was not blocked, which attackers exploited. Successful exploitation of this vulnerability allows attackers to execute arbitrary code on the affected system.
Strike Adobe ColdFusion IPFilterUtils Improper Access Control CVE 2023-38205	CWE: 284 CVE: 2023-38205	This strike exploits an improper access control vulnerability in Adobe ColdFusion. The vulnerability is due to improper validation of the URL path by the IPFilterUtils class which was supposed to block access to sensitive endpoints if accessed from an IP address not from the allow list. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted requests with extra characters to the target server. Successful exploitation could result in access to the ColdFusion Administrator endpoints.
Strike Qlik Sense Path Traversal	CWE: 22 CVE: 2023-41266	This strike exploits a path traversal vulnerability in Qlik sense. A remote, unauthenticated attacker can exploit this by creating an anonymous session and sending maliciously crafted HTTP requests. Successful exploitation could allow the attacker to send further requests to unauthorized endpoints.
Strike Netgate pfSense Command Injection in GIF-GRE Interface Configuration	CVE: 2023-42326	This strike exploits a command injection vulnerability in Netgate pfSense. The vulnerability resides in the improper input validation of parameters in the interfaces_gif_edit.php and interfaces_gre_edit.php files. A remote, authenticated attacker could leverage this flaw by sending specially crafted HTTP POST requests, leading to the execution of arbitrary commands with root privileges.

Name	References	Description
Strike JetBrains TeamCity XML-RPC Authentication Bypass Vulnerability	CWE: 288 CVE: 2023-42793	This strike exploits an authentication bypass vulnerability in JetBrains TeamCity. The vulnerability is due to improper handling of requests using XML-RPC with the "/RPC2" suffix in the Request-URI, which bypasses authentication. Exploiting this vulnerability enables attackers to gain administrator-level access by sending crafted requests to the target server. With elevated privileges, attackers can execute arbitrary commands under the security context of the target server. *Note : While running the strike in one-arm mode, it creates a file /tmp/test on the target server.
Strike Nextgen Mirth Connect XStreamSerializer Insecure Deserialization Vulnerability	CWE: 502 CVE: 2023-43208	This strike exploits an insecure deserialization vulnerability in Nextgen Mirth Connect. This vulnerability is due to improper input validation of XML request body data. The vulnerability exploits the insecure usage of the Java XStream library to unmarshal XML payloads. This improper handling allows attackers to craft malicious XML payloads that can bypass security checks and execute code on the server. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successfully exploiting this vulnerability could result in remote code execution in the security context of SYSTEM. *NOTE : While running the strike as one-arm, the file /tmp/test gets created on the target server.
Strike Ivanti Avalanche FileStoreConfig Arbitrary FileUpload Vulnerability	CVE: 2023-46263 CWE: 434	This strike exploits an arbitrary file upload vulnerability in Ivanti Avalanche. The vulnerability is due to inadequate validation of the txtUncPath field in the Central FileStore configuration settings. A remote authenticated attacker can exploit this by setting the file storage path to target unauthorized directories, specifically the RemoteControl server's webroot. The insufficient checks allow the attacker to bypass blacklist restrictions, enabling malicious files to be uploaded and executed as SYSTEM on the server. Successful exploitation of this vulnerability could lead to remote code execution in the context of the user using the vulnerable server.
Strike Ivanti Connect Secure and Policy Secure Gateways Authentication Bypass	CWE: 287 CVE: 2023-46805	This strike exploits an authentication bypass vulnerability has been reported in Ivanti Connect Secure (formerly Pulse Secure) and Ivanti Policy Secure Gateways. This vulnerability is do to insufficient validation of HTTP request paths in the web process. A remote, unauthenticated attacker can exploit this vulnerability by using one of the Request-URI prefixes and pivoting to a second endpoint. Successful exploitation could result in unauthenticated access to some authenticated REST API endpoints.
Strike QNAP VioStor NVR OS command injection	CWE: 78 CVE: 2023-47565	This strike exploits an OS command injection vulnerability in QNAP VioStor NVR models running QVR Firmware 4.x. The vulnerability is due to improper validation of user-supplied data. A remote, authenticated attacker can exploit this vulnerability by submitting a crafted request to the target server. Successful exploitation could result in remote code execution in the context of the running sever.

Name	References	Description
Strike Apache OFBiz XMLRPC Insecure Deserialization CVE 2023-49070	CWE: 94 CVE: 2023-49070	This strike exploits an insecure deserialization vulnerability in Apache OFBiz. This vulnerability is due to the unmaintained XML-RPC library which deserializes user data. A remote, unauthenticated attacker could exploit this vulnerability by sending a request to the server with an encoded or unnormalized request URI to the "xmlrpc" endpoint, an empty USERNAME or PASSWORD parameter with a parameter requirePasswordChange with a value of Y, and a crafted Java object in a serializable XML element. Successfully exploiting this vulnerability could result in remote code execution in the security context of the user running the OFBiz server.
Strike ownCloud Graph API Information Disclosure Vulnerability	CWE: 22 CVE: 2023-49103	This strike exploits an information disclosure vulnerability in the ownCloud Graph API extension. The vulnerability exists because the affected versions rely on a third-party GetPhpInfo.php library that exposes the secrets stored in environment variables. This flaw allows attackers to steal sensitive information like admin passwords, mail server credentials, and license keys. A remote attacker could exploit the vulnerability by sending a crafted request to the target service. Successful exploitation could result in the disclosure of sensitive information.
Strike Apache Struts HttpParameters.java Unrestricted File Upload	CWE: 552 CVE: 2023-50164	This strike exploits a directory traversal vulnerability in Apache Struts framework. The vulnerability is due to insufficient validation of HTTP parameters during file uploads to the "upload.action" endpoint, resulting in unrestricted file uploads. The vulnerability allows an attacker to manipulate file upload parameters to enable path traversal and upload a malicious file to the target server leading to remote code execution, gaining full system control. *NOTE: While running the strike in one-arm mode, poc.txt file gets created in the /tmp directory of the vulnerable server.
Strike Apache OFBiz Authentication Bypass	CWE: 918 CVE: 2023-51467	This strike exploits an authentication bypass vulnerability in Apache OFBiz. This vulnerability is due to improper input validation of the credentials by the checkLogin function. A remote, unauthenticated attacker could exploit this vulnerability by sending a request with null or invalid username and password parameters and the requirePasswordChange parameter as Y to the server. Successfully exploiting this vulnerability could result in remote code execution in the security context of the web server running the vulnerable application.
Strike Apache Kafka Groovy Script Remote Code Execution	CWE: 94 CVE: 2023-52251	This strike exploits a command injection vulnerability in the web component of Apache Kafka. The vulnerability is due to unrestricted Groovy script execution within the smart filter functionality. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request and might result in arbitrary command execution under the security context of the kafkaui user.
Strike WordPress Backup Migration Plugin Remote Code Execution Vulnerability	CVE: 2023-6553	This strike exploits a remote code execution vulnerability in the WordPress Backup Migration plugin. The vulnerability arises from improper input validation in the backup-heart.php script. A remote, unauthenticated attacker could leverage this flaw by sending a specially crafted HTTP POST request, potentially leading to the execution of arbitrary PHP code on the target server.

Name	References	Description
Strike MLflow get-artifact Local File Read Vulnerability	CWE: 29 CVE: 2023-6909	This strike exploits a Local File Inclusion (LFI) vulnerability in the MLflow framework, which is hosted in the GitHub repository mlflow/mlflow. MLflow is a platform designed to streamline machine learning development, including tracking experiments, packaging code into reproducible runs, and sharing and deploying models. The vulnerability arises from improper handling of URL paths containing directory traversal characters when associating runs with experiments, allowing remote unauthenticated attackers to read arbitrary files on the server. The issue arises from a URI parsing confusion, which allows attackers to manipulate the artifact_location parameter during the creation of an experiment. This can lead to the unintended inclusion of sensitive files like /etc/passwd. Successful exploitation could result in the disclosure of sensitive information.
Strike Palo Alto Networks PAN-OS Management Interface Authentication Bypass	CWE: 306 CVE: 2024-0012	This strike exploits a Authentication Bypass vulnerability in Palo Alto Networks PAN-OS. The vulnerability is due to missing authentication to a critical path. A remote, unauthenticated attacker can exploit by sending a crafted HTTP request to the management web interface. Successful exploitation could result in information disclosure.
Strike Centreon Web updateDirectory SQL Injection Vulnerability	CVE: 2024-0637	This strike exploits an SQL injection vulnerability in the Centreon Web module. The vulnerability exists due to improper input validation in the updateDirectory function when processing the dir_id parameter. A remote, authenticated attacker could leverage this flaw by sending a specially crafted request, leading to arbitrary SQL command execution on the target database.
Strike Atlassian Confluence Data Center and Server addlanguage Remote Code Execution	CWE: 94 CVE: 2024-21683	This strike exploits a remote code execution vulnerability in the Confluence Data Center and Server. The vulnerability is due to insufficient input validation in the function that allows users to add new code block macro language definitions. This flaw allows an authenticated attacker to inject and execute arbitrary Java code by uploading a malicious language file. A remote, authenticated attacker could leverage this vulnerability to inject Java code, resulting in arbitrary code execution under the security context of the user running the vulnerable application. *Note : While running the strike in one-arm mode, it creates a file /tmp/test on the target server.
Strike Ivanti Connect Secure and Policy Secure Gateways Command Injection	CWE: 77 CVE: 2024-21887	This strike exploits a command injection vulnerability in the web components of Ivanti Connect Secure and Ivanti Policy Secure Gateways. This vulnerability is due to the insufficient validation of HTTP arguments. In the web application, two different paths are susceptible to system command injection. The user-submitted data is directly employed in the Python Popen function without undergoing any sanitization. Consequently, an attacker can inject ";command;" and execute shell commands. A remote authenticated attacker could exploit this vulnerability by sending a crafted request to a target server. Successful exploitation could result in arbitrary shell command execution under the security context of the root user.

Name	References	Description
Strike Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery Vulnerability	CWE: 918 CVE: 2024-21893	This strike exploits a Server Side Request Forgery (SSRF) vulnerability in the SAML component of Ivanti Connect Secure, Ivanti Policy Secure, and Ivanti Neurons. The vulnerability arises from insufficient validation of XML content processed by the SAML server, which utilizes an outdated xmltooling library. The URI attribute of the RetrievalMethod element of the XML SOAP allows requests for remote resources via an HTTP GET request, leading to SSRF attacks. A remote, unauthenticated attacker could exploit this vulnerability to access restricted resources. This vulnerability when chained with CVE-2024-21887 may lead to remote code execution.
Strike Centreon Web updateLCARelation SQL Injection Vulnerability	CVE: 2024-23116	This strike exploits an SQL injection vulnerability in the Centreon Web module. The vulnerability exists due to insufficient input validation in the updateLCARelation function when processing the acl_r_topos parameter. A remote, authenticated attacker could leverage this flaw to execute arbitrary SQL commands on the target server's database.
Strike Centreon Web updateContactServiceCommands SQL Injection Vulnerability	CVE: 2024-23117	This strike exploits an SQL injection vulnerability in the Centreon Web module. The vulnerability exists due to insufficient input validation in the updateContactServiceCommands function when processing the contact_svNotifCmds[] parameter. Exploiting this vulnerability allows a remote, authenticated attacker to execute arbitrary SQL commands on the target database, potentially compromising its integrity and security.
Strike Windows CreateProcess cmd.exe Command Injection Vulnerability	CWE: 78 CVE: 2024-24576 CVE: 2024-1874 CVE: 2024-3566	This strike exploits a command injection vulnerability in Windows. The vulnerability arises from improper escaping of arguments when invoking batch files ('bat' and 'cmd' extensions) by the standard libraries across various programming languages. As a result, the Windows command shell (cmd.exe) can be manipulated into executing malicious code. Multiple CVEs are tied to this vulnerability (CVE-2024-24576, CVE-2024-3566, CVE-2024-1874, CVE-2024-22423), however, they all exploit the same underlying weakness. A remote, unauthenticated attacker could exploit this vulnerability by controlling the arguments passed to the spawned process. Successful exploitation could lead to the execution of arbitrary shell commands, bypassing the escaping mechanism, and operating within the security context of the target server.
Strike JetBrains TeamCity BaseController Authentication Bypass Vulnerability	CWE: 288 CVE: 2024-27198	This strike exploits an authentication bypass vulnerability in JetBrains TeamCity. The vulnerability is due to an authentication weakness in the BaseController class, which allows unauthenticated users to access restricted endpoints. It results from inadequate validation of parameters such as the "jsp" parameter and the ".jsp" extension in URLs. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in an attacker bypassing the server's authentication mechanisms, in the worst case, leading to remote code execution under the security context of the target server.

Name	References	Description
Strike Ivanti Endpoint Manager (EPM) xp_cmdshell SQL Injection Vulnerability	CWE: 89 CVE: 2024-29824	This strike exploits an SQL injection vulnerability in Ivanti Endpoint Manager (EPM). The vulnerability lies in the RecordGoodApp() function, where an unsanitized md5 value provided by the user is used in an SQL query. Attackers can exploit this by sending a crafted SOAP request, injecting SQL commands, such as xp_cmdshell, to execute malicious code. Successful exploitation of this vulnerability could allow an unauthenticated attacker within the same network to execute arbitrary code.
Strike D-Link nas_sharing Hardcoded Credentials	CVE: 2024-3272 CWE: 798	This strike exploits an authentication bypass vulnerability in D-Link NAS sharing. The vulnerability is due to the use of hardcoded credentials in nas_sharing. By sending a crafted request, an attacker can bypass authentication.
Strike Apache OFBiz Directory Traversal Vulnerability	CVE: 2024-36104	This strike exploits a directory traversal vulnerability in Apache OFBiz. The vulnerability exists due to improper validation of URL data when processing HTTP requests. A remote, unauthenticated attacker can leverage this flaw by sending specially crafted requests, potentially bypassing authentication or executing arbitrary OS commands on the affected server.
Strike Veertu Anka Build Directory Traversal Vulnerability	CVE: 2024-41163	This strike exploits a directory traversal vulnerability in Veertu Anka Build. The vulnerability exists due to insufficient validation of the "service" parameter in the archive API endpoint. A remote, unauthenticated attacker could leverage this flaw by sending a specially crafted request, enabling them to access and read arbitrary files from the target server.
Strike Mitel MiCollab Path Traversal Vulnerability	CWE: 22 CVE: 2024-41713	This strike exploits a path traversal vulnerability in Mitel MiCollab. A remote unauthenticated attacker can conduct a path traversal attack due to insufficient input validation. Successful exploitation could allow unauthorized access, and the ability to read arbitrary files on the server.
Strike Apache OFBiz Forced Browsing Vulnerability	CWE: 425 CVE: 2024-45195	This strike exploits a forced browsing vulnerability in Apache OFBiz. The vulnerability is due to improper access control in the web application. A remote attacker could exploit this vulnerability by sending a crafted HTTP POST request to the targeted server. Successful exploitation could result in unauthorized access to sensitive information.
Strike Aviatrix Controller OS Command Injection Vulnerability	CVE: 2024-50603 CWE: 78	This strike exploits an OS command injection vulnerability in Aviatrix Controller. The vulnerability allows unauthenticated remote attackers to inject shell metacharacters into the /v1/api endpoint via the cloud_type parameter in list_flightpath_destination_instances or the src_cloud_type parameter in flightpath_connection_test. Successful exploitation of the vulnerability allows remote attackers to execute arbitrary commands on the affected system.

Name	References	Description
Strike Cleo Harmony VLTrader Lexicom File Upload Vulnerability	CVE: 2024-50623 CWE: 434	This strike exploits a file upload vulnerability in Cleo Harmony, VLTrader, Lexicom. The vulnerability allows unauthenticated attackers to upload malicious files, which can then be exploited via directory traversal to execute arbitrary code. Successful exploitation of this vulnerability allows remote attackers to access sensitive information, modify data, or disrupt system operations.
Strike Apache Struts FileuploadIntercept or Unrestricted File Upload	CWE: 434 CVE: 2024-53677	This strike exploits a file upload vulnerability in Apache Struts 2 framework. The vulnerability lies in the File Upload Interceptor, which allows attackers to exploit improperly sanitized file names containing path traversal sequences. This can lead to arbitrary file writes, enabling remote code execution (RCE) in vulnerable applications. The exploitation involves manipulating field name capitalization in file upload forms to bypass Struts 2's parameter binding, allowing attackers to control internal variables like top.uploadFileName via the OGNL value stack. Exploitation is customized, requiring knowledge of the upload endpoint's structure.
Strike Ivanti Cloud Services Appliance OS Command Injection Vulnerability	CWE: 78 CVE: 2024-8190	This strike exploits an OS command injection vulnerability in the Ivanti Cloud Services Appliance, versions prior to 4.6 Patch 519. This vulnerability is due to improper validation of user data sent to the datetime php endpoint. Successful exploitation might result in arbitrary code execution in the context of the root user.
Strike Ivanti Cloud Services Appliance broker Authentication Bypass	CWE: 22 CVE: 2024-8963	This strike exploits Authentication Bypass vulnerability in Ivanti Cloud Services Appliance. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted requests to the target server. Successful exploitation could allow an unauthorized attacker to access restricted functionality.
Strike Docker Daemon API Unauthorized Remote Code Execution		This strike exploits a remote code execution vulnerability in Docker daemon API. An attacker can start a docker container, attach host's /etc to the container and read/write files in etc.
Strike TOPSEC Firewall ELCO ELIGIBLECONTESTANT Remote Code Execution	EXPLOITDB : 40272	This strike emulates a remote code execution attack against TopSec Firewalls. This attack uploads and executes arbitrary code via an HTTP POST request to /cgi/maincgi.cgi. NOTE: By default the vulnerable services are accessed via SSL connection (port 443). A publicly available exploit for this vulnerability can be found in the reported leak of 0Day exploits from the NSA by a group known as the "Shadow Brokers", identified as ELIGIBLECONTESTANT
Strike TOPSEC Firewall ELCA ELIGIBLECANDIDATE Remote Code Execution	EXPLOITDB : 40273	This strike emulates a remote code execution attack against TopSec Firewalls. This attack uploads and executes arbitrary code via an HTTP POST request to /cgi/maincgi.cgi. NOTE: By default the vulnerable services are accessed via SSL connection (port 443). A publicly available exploit for this vulnerability can be found in the reported leak of 0Day exploits from the NSA by a group known as the "Shadow Brokers", identified as ELIGIBLECANDIDATE.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike WordPress Quizlord plugin Reflected Cross Site Scripting	EXPLOITDB : 45307	This strike exploits a reflected cross-site scripting vulnerability found in Quizlord WordPress plugin. This vulnerability is due to inadequate input filtering in the web interface, while parsing input passed to quiz title parameter. By exploiting this vulnerability an attacker could cause arbitrary HTML/script code to be executed by the target user's browser.
Strike Firefox Hyphenated URL Exploit Variant 2	BID: 14784 CVE: 2005-2871	This strike exploits a flaw in the Firefox browser that is triggered by a hostname in a URL that is all hyphens.
Strike Adobe Flash 9-10 ASnative(15,0) NULL Pointer Dereference		This strike exploits a NULL pointer dereference in the Adobe Flash browser plugin. This flaw is triggered when the ASnative method is used to call function 15-0 with a string as the first parameter.
Strike Adobe Flash 9-10 ASnative(301,1) NULL Pointer Dereference		This strike exploits a NULL pointer dereference in the Adobe Flash browser plugin. This flaw is triggered when the ASnative method is used to call function 301-1 with less than two parameters.
Strike HP Intelligent Management Center Unauthenticated File Retrieval		This strike exploits a directory traversal vulnerability presents in the HP Intelligent Management Center. The vulnerability is due to insufficient validation of traverse directory requests. The remote attacker may disclosure the information in the target system.
Strike Headline Portal Engine page.newnews.show.php3 HPEinc Parameter PHP File Include	BID: 19663	This strike exploits a PHP include flaw in the Headline Portal Engine web application. An attacker could exploit this vulnerability to execute arbitrary server-side script code.
Strike Headline Portal Engine thememaker.php3 HPEinc Parameter PHP File Include Variant 2	BID: 19663	This strike exploits a PHP include flaw in the Headline Portal Engine web application. An attacker could exploit this vulnerability to execute arbitrary server-side script code.
Strike IBM Lotus Sametime StMux.exe Buffer Overflow	CWE: 119 CVE: 2008-2499 BID: 29328	This strike triggers a stack buffer overflow in IBM Lotus Sametime Server (StMux.exe) by doing a POST request with an overly long path.
Strike Internet Explorer AxDebugger.Document DoS		This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the AxDebugger.Document COM object.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike CapiCom.Utilities ActiveX GetRandom Integer Overflow Denial of Service		This strike causes a denial of service in Microsoft's CapiCom.Utilities ActiveX Control by exploiting an integer overflow in the 'GetRandom' function.
Strike Internet Explorer HtmlDlgSafeHelper.HtmlDlgSafeHelper.BlockFormats DoS		This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the HtmlDlgSafeHelper.HtmlDlgSafeHelper COM object.
Strike Internet Explorer Internet.PopupMenu.RemoveItem DoS		This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the Internet.PopupMenu COM object.
Strike Internet Explorer OutlookExpress.AddressBook DoS	CWE: 119 CVE: 2005-4840	This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the OutlookExpress.AddressBook COM object.
Strike Internet Explorer Sysmon DoS		This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the Sysmon COM object.
Strike Microsoft IIS 5.0 ISAPI .printer Extension Host Header Overflow Variant 2	CVE: 2001-0241 BID: 2674	This strike exploits a buffer overflow in the .printer ISAPI extension for Microsoft IIS 5.0 when handling long Host HTTP headers.
Strike Liquid XML Studio 2010 OpenFile() ActiveX Buffer Overflow		This strike exploits a buffer overflow vulnerability present in the OpenFile() method of the LtXmlComHelp8.dll ActiveX control included with Liquid XML Studio 2010.
Strike IBM Lotus Domino HTTP Header Accept-Language Buffer Overflow	CWE: 119 CVE: 2008-2240 BID: 29310	This strike exploits a buffer overflow flaw in the IBM Lotus Domino web server. If a specially formatted URI is requested in combination with an overly long Accept-Language value, the flaw will be triggered, possibly allowing an attacker to execute arbitrary code.
Strike IBM Lotus Domino HTTP Redirect Buffer Overflow	CVE: 2003-0178 BID: 6870	This strike exploits a buffer overflow flaw in the IBM Lotus Domino web server.
Strike MagnetoSoft ICMP AddDestinationEntry ActiveX Control Buffer Overflow		This module exploits a buffer overflow in the MagnetoSoft ICMP AddDestinationEntry ActiveX Control.

Name	References	Description
Strike Operation Quicksand Nov 2020 Campaign - Powershell Malware File Transfer	MD5: 2e7b4ae4b aa70458824 8b425b8e02 7bf  SHA1: 60b5b41bd5 98fd844630 fdf609539fc 854437392  SHA256: 8bbcd7013 e339cca41c f85a0788ef0 fc250b5451 5a038eff6d4 838a16be04 7d7	This strike simulates the download of the Powershell malware via an HTTP GET request.
Strike McAfee EPolicy Orchestrator Source Header Overflow	BID: 20288  CVE: 2006-5156	This strike exploits buffer overflow in the EPolicy Orchestrator HTTP service.
Strike Microsoft Visual FoxPro 6 fpole.ocx FoxDoCmd ActiveX Command Execution	BID: 25977  CWE: 78  CVE: 2007-5322	This strike exploits an input sanitization flaw in Microsoft Visual FoxPro 6 that allows arbitrary commands to be executed by the FoxDoCmd method of the fpole.ocx ActiveX control.
Strike Microsoft Windows Media Services Logging ISAPI Buffer Overflow (121)	  CVE: 2003-0227  BID: 7727	This strike exploits a stack-based buffer overflow in Microsoft Windows Media Services via a 121 byte POST to nsiislog.dll which results in remote code execution.
Strike Microsoft Windows Media Services Logging ISAPI Buffer Overflow (5000)	  CVE: 2003-0227  BID: 7727	This strike exploits a stack-based buffer overflow in Microsoft Windows Media Services via a 5000 byte POST to nsiislog.dll which results in remote code execution.
Strike Microsoft Windows Media Services Logging ISAPI Buffer Overflow (510)	  CVE: 2003-0227  BID: 7727	This strike exploits a stack-based buffer overflow in Microsoft Windows Media Services via a 510 byte POST to nsiislog.dll which results in remote code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Windows Compressed Folder Exploit Download (HTTP)	CVE: 2004-0575	This strike exploits a vulnerability in Microsoft Windows when opening a zip file containing a file with a long filename. This strike simulates downloading a malicious zip file via HTTP.
Strike Microsoft Internet Explorer Install Engine SetCifFile Heap Overflow	CVE: 2004-0216 BID: 11366	This strike exploits a heap buffer overflow in the Microsoft Internet Explorer Install Engine ActiveX control.
Strike Microsoft Internet Explorer WMSpecialEffectDX T2Inputs.bstrProper tyName Memory Corruption	CWE: 94 CVE: 2006-1303 BID: 18328	This strike exploits a vulnerability in Microsoft Internet Explorer when instantiating the wmm2fxa.dll component.
Strike Microsoft Visio File Version Code Execution (HTTP)		This strike exploits an arbitrary code execution flaw in Microsoft Visio 2002. The vulnerability is triggered when a version is specified that is less than six and greater than zero.
Strike Microsoft Windows PDF URI Handling Arbitrary Command Execution (HTTP)	CWE: 94 CVE: 2007-5020 BID: 25748	This strike exploits a command execution vulnerability in Microsoft Windows XP and 2003 URI handling via the Adobe Acrobat 8.x PDF (.pdf) "mailto" URI object's resolving functionality when paired with IE7 as the default URI handler.
Strike Internet Explorer - Snapshot Viewer for Microsoft Access ActiveX Arbitrary File Download Variant 2	CWE: 94 CVE: 2008-2463 BID: 30114	This strike exploits a malicious instantiation of the Snapshot Viewer for Microsoft Access ActiveX control. Due to a design error, a malicious web page may silently download executable files from an Internet site to any location on the victim's hard drive, including auto-start extensibility points (ASEPs). These programs, in turn, may then silently run with the privileges of the currently-logged on user.
Strike Internet Explorer - Snapshot Viewer for Microsoft Access ActiveX Arbitrary File Download Variant 3	CWE: 94 CVE: 2008-2463 BID: 30114	This strike exploits a malicious instantiation of the Snapshot Viewer for Microsoft Access ActiveX control. Due to a design error, a malicious web page may silently download executable files from an Internet site to any location on the victim's hard drive, including auto-start extensibility points (ASEPs). These programs, in turn, may then silently run with the privileges of the currently-logged on user.
Strike ISA Server 2006 XSS in CookieAuth.dll	CWE: 79 CVE: 2009-0237	A cross-site scripting vulnerability exists in Microsoft ISA Server 2006.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Embedded OpenType Font Parser Code Execution (HTTP)	CWE: 119 CVE: 2009-0231	This strike exploits a vulnerability in Microsoft's Embedded OpenType file parsing engine when parsing an EOT file containing malicious OpenType font file structure data.
Strike Microsoft ASP.NET Request Scheduling DoS	BID: 35985 CWE: 20 CVE: 2009-1536	This strike exploits a DoS bug in the Microsoft .NET Framework via IIS with ASP.NET configured to use integrated mode.
Strike Microsoft Outlook Web Components ActiveX Spreadsheet Control Overflow	CWE: 119 CVE: 2009-1534 BID: 35992	This strike exploits a stack overflow with an SEH overwrite in the Outlook Web Components Spreadsheet ActiveX Control. The HTMLURL property is used as the attack vector delivered via HTML/JavaScript code rendered in Internet Explorer.
Strike Windows Media Player ASF Media File Format Parsing Code Execution (HTTP)	CWE: 119 CVE: 2009-2527	This strike exploits a code execution vulnerability in Microsoft Windows Media Player 6.4 when parsing an Advanced System Format (.ASF/.WMV/.WMA) file containing a Header Extension Object which contains a Index Object with an overly large IndexEntriesCount value.
Strike Windows Media Player ASF Media File Format Header Extension Parsing Code Execution (HTTP)	CWE: 119 CVE: 2009-2527	This strike exploits a code execution vulnerability in Microsoft Windows Media Player 6.4 when parsing an Advanced System Format (.ASF/.WMV/.WMA) file containing a Header Extension Object which contains a Marker Object with an overly large MarkersCount value.
Strike Microsoft Embedded OpenType Font Parser Directory Entry Summed Length & Offset Integer Wrap Code Execution (HTTP)	CWE: 94 CVE: 2009-2514	This strike exploits a vulnerability in Microsoft's Embedded OpenType file parsing engine when parsing an EOT file containing a directory entry where the directory entry's length and offset summed cause an integer wrap. This wrapped integer is then subsequently used to allocate memory for the directory. When the directory data is then written to the allocated buffer, it is overflowed resulting in heap corruption and control of code execution.
Strike Netscape-iPlanet Search NS-Query-Pat Traversal (Unix)	CVE: 2002-1042 BID: 5191	This strike exploits a directory traversal flaw in search engine provided with the Netscape and iPlanet web servers.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Novell GroupWise Messenger HTTP Response Handling Stack Buffer Overflow	CWE: 119 CVE: 2008-2703 BID: 29602	This strike exploits a stack-based buffer overflow present in Novell GroupWise Messenger (GWIM) Client before 2.0.3 HP1 for Windows which allows remote code execution by way of "spoofed server responses" that contain a long string after the NM_A_SZ_TRANSACTION_ID field name.
Strike Opera JavaScript Alert() Buffer Overflow		This strike exploits a flaw in Opera 10.10 in which overly long values given to the JavaScript Alert() function can cause the browser to crash
Strike Opera 10.53 JavaScript getImageData() Memory Corruption DoS		This strike exploits a flaw in Opera 10.53 in which a malformed call to the JavaScript getImageData() function can cause the browser to crash.
Strike Oracle HTTP Server username XSS Vulnerability	BID: 9484 CVE: 2004-2115	This strike exploits an XSS vulnerability in the Oracle HTTP Server (based on Apache)
Strike Oracle HTTP Server password XSS Vulnerability	BID: 9484 CVE: 2004-2115	This strike exploits an XSS vulnerability in the Oracle HTTP Server (based on Apache)
Strike Oracle HTTP Server action XSS Vulnerability	BID: 9484 CVE: 2004-2115	This strike exploits an XSS vulnerability in the Oracle HTTP Server (based on Apache)
Strike Oracle Java 5,6,7 ZipFile readCEN Denial of Service	BID: 52013 CVE: 2012-0501	This strike exploits an denial of service vulnerability in Oracle Java. The vulnerability is due to a recursion error in the Oracle Java ZipFile class when a malicious zipfile is processed.
Strike Oracle Secure Backup exec_qr() \$ora_osb_bgcookie Command Execution	CVE: 2008-5448 BID: 33177	This strike sends a command execution attack leveraging an unsanitized variable used by Oracle Secure Backup's exec_qr() function.
Strike Oracle Secure Backup exec_qr() \$ora_osb_lcookie Command Execution	CVE: 2008-5448 BID: 33177	This strike sends a command execution attack leveraging an unsanitized variable used by Oracle Secure Backup's exec_qr() function.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle Secure Backups exec_qr() \$rbtool Command Execution	CVE: 2008-5448 BID: 33177	This strike sends a command execution attack leveraging an unsanitized variable used by Oracle Secure Backup's exec_qr() function.
Strike Oracle TimesTen Data Server Log Format String	CVE: 2008-5440 BID: 33177	This strike exploits a format string vulnerability Oracle Database 7.0.5's TimesTen Data Server. An attacker may send a format string to the event viewer, causing the component to either crash or execute malicious code.
Strike SolarWinds Storage Manager AuthenticationFilter Authentication Bypass	BID: 69438	This strike exploits a vulnerability inside SolarWinds Storage Manager which allows bypass of authentication filters. This in turn can lead to arbitrary file upload and code execution on the target server.
Strike WebUI mainfile.php arbitrary command injection		This strike exploits a command injection vulnerability in WebUI. The vulnerability is due to improper validation of user supplied data in mainfile.php. By exploiting this vulnerability, an unauthenticated attacker can execute arbitrary code on the target system.
Strike ManageEngine Applications Manager CommonAPIUtil SyncMonitors SQL Injection		This strike exploits an SQL injection vulnerability in ManageEngine Application Manager. The vulnerability is due to improper validation of user supplied input in the SyncMonitors method. An unauthenticated attacker can exploit this vulnerability by sending crafted HTTP requests to the vulnerable server.
Strike CA Total Defense Suite UNC Management SQL Injection		This strike exploits a SQL injection vulnerability within CA Total Defense Suite. This vulnerability is due to improper sanitation of parameters in a procedure. A remote attacker can take advantage of this vulnerability to inject SQL commands.
Strike PHP POST File Upload PHP GLOBALS Variable Overwrite	CVE: 2005-3390 BID: 15250	This strike exploits a vulnerability in PHP which allows an attacker to overwrite the PHP \$GLOBALS variable when performing a POST operation with a multipart/form-data request.
Strike PHP POST File Upload Overflow	CVE: 2002-0081 BID: 4183	This strike exploits a remote heap overflow in the PHP programming language function php_mime_split.
Strike Microsoft Powerpoint 2003 Heap Overflow (HTTP)		This strike exploits a heap overflow vulnerability in Microsoft Office 2005 Powerpoint

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Redaxo CMS Addon MyEvents 2.2.1 - SQL Injection	EXPLOITDB : 44261	This strike exploits a SQL injection vulnerability in the Redaxo CMS Addon MyEvents. This vulnerability is due to improper sanitization for the parameter "myevents_id". A remote attacker can access backend contents with successful exploitation.
Strike Safari Use-After-Free Parent.Close() Vulnerability	CWE: 399 CVE: 2010-1939 BID: 39990	Safari 4.0.5 and 4.0.4 are vulnerable to a use-after-free exploit that can lead to code execution. Other versions (4.0.X versions prior to 4.0.4) are at least susceptible to denial of service attacks via the same vector. The vulnerability is triggered when a child window stores a reference to its parent, attempts to close the parent, and then tries to access a property/call a function on the parent.
Strike Microsoft Sharepoint 2007 Path Info XSS	BID: 23832  CWE: 79  CVE: 2007-2581	This strike triggers a cross-site scripting vulnerability in the Microsoft Sharepoint 2007 web service.
Strike Skype URI Handler Input Validation Vulnerability	BID: 38699	This strike exploits a vulnerability in the way Skype parses skype-protocol urls, such as skype:user123?call. The vulnerability allows an attacker to pass additional command-line arguments to the Skype executable, which may force the user to persist his/her credentials in a remote location, such as an UNC share.
Strike SolusLabs SolusVM centralbackup.php SQL injection arbitrary command execution		This strike exploits a SQL injection vulnerability with arbitrary command execution in SolusVM. A specially crafted POST request can be sent to an active VM, resulting in arbitrary command execution.
Strike Squid HTTP header buffer overflow	CWE: 119  CVE: 2013-4115  BID: 61111	This strike exploits a buffer overflow vulnerability in Squid. This vulnerability is due to improper handle large header in HTTP request.
Strike NetWin SurgeMail Webmail Server page Parameter Format String	CWE: 134  CVE: 2008-1055  BID: 27990	This strike simulates a format string attack against the NetWin SurgeMail webmail server.
Strike Ultimate PHP Board User-Agent HTTP Header Code Execution	CVE: 2003-0395	This strike exploits a code execution flaw in the Ultimate PHP Board web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike VEGO Web Forum index.php theme_id Parameter SQL Injection Variant 2 (<v1.26)	CVE: 2006-0065 BID: 16107	This strike exploits a SQL injection flaw in the VEGO web forum.
Strike VLC Ogg Vorbis Comment Header Format String (HTTP)	BID: 24555 CVE: 2007-3316	This strike exploits a format string vulnerability in VLC when decoding Ogg Vorbis files. This strike simulates downloading a malicious file via HTTP.
Strike WebBBS webbbs_config.pl followup Parameter Shell Execution	CVE: 2002-1993 BID: 5048	This strike exploits a remote command execution flaw in the WebBBS bulletin board application.
Strike Wireshark Profinet DCP Dissector Name of Station Set Request Format String Vulnerability		This strike triggers a denial of service vulnerability in the Wireshark network protocol analyzer. The method for triggering the vulnerability is to transfer a malicious pcap file over the HTTP protocol.
Strike Word Macro HTTP Exfiltration Macro-enabled VBA Maldoc Command and control		This strike exfiltrates host information via HTTP POST request.
Strike Microsoft WordPad Embedded COM Code Execution (InstallEngine) (HTTP)		This strike exploits a flaw in Microsoft WordPad that can be used to execute arbitrary code. This particular strike embeds the InstallEngine COM control into the OLE section of a WordPad RTF document.
Strike Microsoft WordPad Embedded COM Code Execution (Sysmon.3) (HTTP)		This strike exploits a flaw in Microsoft WordPad that can be used to execute arbitrary code. This particular strike embeds the Sysmon.3 COM control into the OLE section of a WordPad RTF document and defines a set of corrupt OLE properties that will cause a crash on load.
Strike Wordpress Download Manager Plugin Remote File Upload		A remote file upload vulnerability exists in Wordpress Download Manager Plugin versions prior to 2.7.5. This vulnerability allows an unauthenticated attacker to upload a file to the web server and could facilitate remote code execution with the privileges of the account running the web server application.
Strike Wordpress page-flip-image-gallery plugins Remote File Upload		This strike exploits a remote file upload vulnerability inside wordpress page flip image gallery plugin.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike WordPress Property Plugin PHP File Upload Code Execution	BID: 53787	This strike identifies a vulnerability in the WordPress Property plugin. Due to improper validation, a user can upload a file to a temporary directory that will allow for remote code to be executed.
Strike Netscape Server WP Tag Directory Index Variant 8	BID: 1063 CVE: 2000-0236	This strike attempts to obtain a directory listing from the web server by specifying a special request parameter.
Strike Netscape Server WP Tag Directory Index Variant 9	BID: 1063 CVE: 2000-0236	This strike attempts to obtain a directory listing from the web server by specifying a special request parameter.
Strike Joomla Plugin Mod_simplefileupload File Upload		This strike exploits a file upload vulnerability present in Joomla mod_simplefileupload plugin. By exploiting this vulnerability, an unauthenticated attacker can run arbitrary code by uploading files on the server and execute them. Note: This vulnerability was disclosed by the XAttacker tool.
Strike XAttacker Tool Prestashop Addons Arbitrary File Upload		This strike exploits file upload vulnerabilities in Prestashop CMS addons targeted by recently published XAttacker Tool. The main issue is the lack of sanitization of the user-supplied files by the components in charge of handling files upload queries. By exploiting these vulnerabilities, an unauthenticated attacker can run arbitrary code by uploading files on the server and execute them.
Strike XAttacker Tool WordPress Plugins Arbitrary File Upload (verified)	CVE: 2015-2825 EXPLOITDB : 36374 EXPLOITDB : 34922 EXPLOITDB : 36640	This strike exploits a series of file upload vulnerabilities in different Wordpress Plugins targeted by recently published XAttacker Tool. The common issue is the lack of sanitization of the user-uploaded files in the components in charge of handling files upload queries. . By exploiting this vulnerabilities, an unauthenticated attacker can run arbitrary code by uploading files on the server and execute them.
Strike Multiple ManageEngine Products It360SPUtil SQL Injection		This strike exploits an SQL injection vulnerability in ManageEngine Applications Manager and ManageEngine IT360 MSP Edition. The vulnerability is due to improper validation of It360SPUtil resIds HTTP parameter. An attacker could exploit this vulnerability by sending an unauthenticated malicious request to the server, compromising the integrity of the database.
Strike Trend Micro Safe Sync Reconnect Query String Multiple Parameters Command Injection		This strike exploits a command execution vulnerability in Trend Micro Safe Sync. Several query string parameters accepted by the reconnect command are vulnerable to command injection. An authenticated attacker can connect, disconnect, and then send a specially crafted HTTP command to reconnect in order to achieve arbitrary code execution with root privileges.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Trend Micro IWSVA deploywizard haport Parameter Command Injection		This strike exploits a command execution vulnerability in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The haport parameter, which is sent in HTTP GET requests to the /deploywizard/deploywizard.do uri, is vulnerable to command injection and is not sanitized. An attacker can send a specially crafted HTTP GET request to achieve arbitrary command execution. NOTE: By default the vulnerable services are accessed via SSL connection (port 8443)
Strike ZebraFeeds controller.php zf_path Parameter PHP File Include	CVE: 2007-1010 BID: 22576	This strike exploits a PHP include flaw in ZebraFeeds 1.1.
Strike Microsoft SharePoint WSDL DISCO Inifinate Loop Denial of Service	CWE: 20 CVE: 2013-0081 BID: 62205	Microsoft SharePoint contains a denial of service vulnerability. When a non-existent custom web application is requested, the program will enter an infinite loop while searching for the web application, resulting in a denial of service condition.
Strike Arcserve Unified Data Protection Console Multiple Directory Traversal Vulnerabilities	CWE: 22 CVE: 2015-4068 BID: 74845	This strike exploits a directory traversal vulnerability in Arcserve Unified Data Protection prior to version 5.0 update 4. The vulnerability is caused by improper validation of a file path supplied by the user in the export and reportFile servlets. A remote, unauthenticated attacker could exploit this by sending crafted requests to the application, leading to denial-of-service, information disclosure and, possibly, loss of information.
Strike Oracle WebLogic Server Directory Traversal Vulnerability	CVE: 2020-14750 CWE: 22	This strike exploits a directory traversal vulnerability in Oracle WebLogic Server. The vulnerability arises due to improper input validation which allows attackers to bypass authentication mechanisms. A remote, unauthenticated attacker can send crafted HTTP requests containing double encoded directory traversal sequences to access restricted paths such as console.portal without proper authentication. Successful exploitation could lead to remote code execution, potentially resulting in full compromise of the Oracle WebLogic Server.
Strike Sun Java Plugin JNLP Argument Injection (Debug)	BID: 12847  CVE: 2005-0418  CVE: 2005-0836	This strike exploits a flaw in the Sun Java plugin that allows arbitrary code execution through malicious JNLP files.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Sun Java Plugin JNLP Argument Injection (Policy)	BID: 12847  CVE: 2005-0418  CVE: 2005-0836	This strike exploits a flaw in the Sun Java plugin that allows arbitrary code execution through malicious JNLP files.
Strike Apple OS X QuickDraw GetSrcBits32ARGB Memory Corruption Denial of Service (IMAP4)	BID: 22207  CVE: 2007-0462	This strike exploits a denial of service condition in Apple's Mac OS X when opening a malformed PICT file.
Strike Microsoft Excel NULL Pointer DoS (A) (IMAP4)	BID: 22717  CVE: 2007-1239	This strike exploits a denial of service flaw in Microsoft Excel using a corrupted XLS document.
Strike Microsoft Excel NULL Pointer DoS (B) (IMAP4)	BID: 22717  CVE: 2007-1239	This strike exploits a denial of service flaw in Microsoft Excel using a corrupted XLS document.
Strike Chicken of the VNC Hostname Size Denial of Service	CVE: 2007-0756  BID: 22372	This strike causes a denial of service in the Chicken of the VNC client program by specifying a long hostname length field in a VNC server.
Strike Adobe Acrobat Reader getIcon Memory Corruption (IMAP4 Base64)	BID: 34169  CWE: 20  CVE: 2009-0927	This strike exploits a flaw in Adobe's PDF reader that can result in the execution of arbitrary code.
Strike Adobe Acrobat Reader getIcon Memory Corruption (IMAP4 Quoted Printable)	BID: 34169  CWE: 20  CVE: 2009-0927	This strike exploits a flaw in Adobe's PDF reader that can result in the execution of arbitrary code.
Strike GDI+ PNG Integer Overflow Vulnerability (IMAP4 Quoted Printable)	CWE: 189  CVE: 2009-3126	This strike exploits the way the buffer size for the pixel data in interlaced PNGs is calculated by GDI+. The methods used by GDI+ contain integer overflow vulnerabilities.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Windows Media Player ASX File Heap Overflow (IMAP4 Base64)	CWE: 119 CVE: 2006-6134 BID: 21247	Microsoft Windows Media Player contains a vulnerability that will cause memory corruption when a malicious *.asx file is opened
Strike Windows Media Player ASX File Heap Overflow (IMAP4 Quoted Printable)	CWE: 119 CVE: 2006-6134 BID: 21247	Microsoft Windows Media Player contains a vulnerability that will cause memory corruption when a malicious *.asx file is opened
Strike Microsoft Windows AVIFile Media File Truncation Code Execution (IMAP4 Base64)	BID: 35967 CWE: 94 CVE: 2009-1545	This strike exploits a vulnerability in Microsoft Windows when parsing an AVI file with truncated AVIH chunk data.
Strike Digium Asterisk Manager Shell Execution	CWE: 287 CVE: 2012-2414 BID: 53206	This strike exposes an ability for an authenticated user to run an arbitrary shell command without restriction.
Strike Internet Explorer EMF File Rendering Denial of Service (IMAP4)	CWE: 399 CVE: 2005-0803 BID: 12834	This strike exploits a denial of service flaw in Microsoft Windows. This flaw is triggered through a malformed Windows EMF Metafile. This strike simulates downloading an EMF file via IMAP4.
Strike Microsoft Windows LoadImage API Overflow (IMAP4)	BID: 12095 CVE: 2004-1049	This strike exploits a flaw in the parsing of images via LoadImage on Microsoft Windows. This strike simulates downloading a malicious .ani animated cursor in an IMAP4 message.
Strike MWindows Mail HTML Link Program Execution (IMAP4)	BID: 23103 CVE: 2007-1658	This strike exploits an arbitrary program execution flaw in the Windows Mail client. This flaw is triggered when a user clicks a hyperlink within an HTML email.

Name	References	Description
Strike MWindows Mail HTML Link Program Execution UNC (IMAP4)	BID: 23103  CVE: 2007-1658	This strike exploits an arbitrary program execution flaw in the Windows Mail client. This flaw is triggered when a user clicks a hyperlink within an HTML email.
Strike Microsoft Windows Vista Contact Gadget Remote Code Execution (IMAP4)	CVE: 2007-3032  BID: 25304	This strike exploits a flaw in the Contact Gadget in Microsoft Vista when displaying a malicious contact.
Strike Microsoft Word RTF Object Parsing Vulnerability (dpendgroup) (IMAP4 Base64)	CWE: 399  CVE: 2008-4030	This strike exploits a vulnerability in MS Word caused by an RTF file with invalid 'dpendgroup' directives.
Strike UNIX rlogind Service -root Authentication Bypass	CVE: 1999-0113  BID: 458	This strike exploits an authentication bypass vulnerability present in certain versions of the rlogin service.
Strike Microsoft Windows SMB NT Rename Buffer Overflow	CWE: 20  CVE: 2017-0146  BID: 96707	This strike exploits a buffer overflow vulnerability in Microsoft Windows SMB Service. The vulnerability can be triggered by sending an overly large NT Trans request. A remote, unauthenticated attacker could exploit this vulnerability to execute arbitrary code on the target system. * NOTE: This vulnerability was targeted with ShadowBrokers EternalChampion exploit
Strike Microsoft Windows SMB Information Disclosure	CWE: 200  CVE: 2017-0147  BID: 96709	This strike exploits an information disclosure vulnerability in Microsoft Windows SMB Service. The vulnerability can be triggered by sending an SMB request that reads beyond a boundary. A remote, unauthenticated attacker could exploit this vulnerability to reveal memory addresses for use with other exploits. * NOTE: This vulnerability was targeted with ShadowBrokers EternalChampion exploit
Strike SSLv2 DROWN decryption	CWE: 200  CVE: 2016-0800  CVE: 2016-0703	This strike simulates traffic which may be seen during the man-in-the-middle DROWN SSLv2 decryption attack. In order to gather enough data to break encryption, an attacker may initiate several thousand SSLv2 handshakes. This strike initiates only 100 handshakes to reduce test time, however, because the recommended remediation is to completely disable SSLv2, even one handshake should be viewed as suspicious.

Name	References	Description
Strike Cisco NX-OS Command Injection	BID: 50347 CWE: 264 CVE: 2011-2569	This strike exploits a vulnerability in the input sanitization of Cisco's NX-OS which allows for command injection when output is piped to certain commands (less, section). This can be used to achieve privilege escalation.
Strike Oracle WebLogic Server Insecure Deserialization - RCE	CWE: 502 CVE: 2018-2628 BID: 103776	An insecure deserialization vulnerability was found in Oracle WebLogic Server due to insufficient validation of serialized data. Vulnerability can be exploited by sending a specially crafted serialized object. Successful exploitation can result in arbitrary code execution in the context of the user running WebLogic.
Strike AI LLM Database Create Operation - Gemini		This strike sends a prompt to manipulate the Gemini LLM into generating a database-level CREATE operation. The request is designed to trigger the LLM into producing a SQL query that performs schema creation tasks, such as creating new tables, schemas or databases. The LLM's response includes a full SQL CREATE statement which, if executed, could result in unauthorized database changes or setup of malicious data structures. Target LLM: Gemini
Strike AI LLM Database Create Operation - Grok		This strike sends a prompt to manipulate the Grok LLM into generating a database-level CREATE operation. The request is designed to trigger the LLM into producing a SQL query that performs schema creation tasks, such as creating new tables, schemas or databases. The LLM's response includes a full SQL CREATE statement which, if executed, could result in unauthorized database changes or setup of malicious data structures. Target LLM: Grok
Strike AI LLM Database Create Operation - OpenAI		This strike sends a prompt to manipulate the OpenAI LLM into generating a database-level CREATE operation. The request is designed to trigger the LLM into producing a SQL query that performs schema creation tasks, such as creating new tables, schemas or databases. The LLM's response includes a full SQL CREATE statement which, if executed, could result in unauthorized database changes or setup of malicious data structures. Target LLM: OpenAI
Strike AI LLM Database Delete Operation - Gemini		This strike sends a prompt to manipulate the Gemini LLM into generating a database-level DELETE operation. The request is designed to trigger the LLM into producing a SQL query that performs data deletion tasks, such as deleting records from tables or removing specific data entries. The LLM's response includes a full SQL DELETE or DROP statement which, if executed, could result in unauthorized data loss or corruption of the database. Target LLM: Gemini
Strike AI LLM Database Delete Operation - Grok		This strike sends a prompt to manipulate the Grok LLM into generating a database-level DELETE operation. The request is designed to trigger the LLM into producing a SQL query that performs data deletion tasks, such as deleting records from tables or removing specific data entries. The LLM's response includes a full SQL DELETE or DROP statement which, if executed, could result in unauthorized data loss or corruption of the database. Target LLM: Grok

Name	References	Description
Strike AI LLM Database Delete Operation - OpenAI		This strike sends a prompt to manipulate the OpenAI LLM into generating a database-level DELETE operation. The request is designed to trigger the LLM into producing a SQL query that performs data deletion tasks, such as deleting records from tables or removing specific data entries. The LLM's response includes a full SQL DELETE or DROP statement which, if executed, could result in unauthorized data loss or corruption of the database. Target LLM: OpenAI
Strike AI LLM Database Read Operation - Gemini		This strike sends a prompt to manipulate the Gemini LLM into generating a database-level READ operation. The request is designed to trigger the LLM into producing a SQL query that performs data retrieval tasks, such as selecting data from tables or querying specific information. The LLM's response includes a full SQL SELECT statement which, if executed, could result in unauthorized data access or exposure of sensitive information. Target LLM: Gemini
Strike AI LLM Database Read Operation - Grok		This strike sends a prompt to manipulate the Grok LLM into generating a database-level READ operation. The request is designed to trigger the LLM into producing a SQL query that performs data retrieval tasks, such as selecting data from tables or querying specific information. The LLM's response includes a full SQL SELECT statement which, if executed, could result in unauthorized data access or exposure of sensitive information. Target LLM: Grok
Strike AI LLM Database Read Operation - OpenAI		This strike sends a prompt to manipulate the OpenAI LLM into generating a database-level READ operation. The request is designed to trigger the LLM into producing a SQL query that performs data retrieval tasks, such as selecting data from tables or querying specific information. The LLM's response includes a full SQL SELECT statement which, if executed, could result in unauthorized data access or exposure of sensitive information. Target LLM: OpenAI
Strike AI LLM Database Update Operation - Gemini		This strike sends a prompt to manipulate the Gemini LLM into generating a database-level UPDATE operation. The request is designed to trigger the LLM into producing a SQL query that performs data modification tasks, such as updating existing records in a database. The LLM's response includes a full SQL UPDATE statement which, if executed, could result in unauthorized data changes or corruption of existing information. Target LLM: Gemini
Strike AI LLM Database Update Operation - Grok		This strike sends a prompt to manipulate the Grok LLM into generating a database-level UPDATE operation. The request is designed to trigger the LLM into producing a SQL query that performs data modification tasks, such as updating existing records in a database. The LLM's response includes a full SQL UPDATE statement which, if executed, could result in unauthorized data changes or corruption of existing information. Target LLM: Grok
Strike AI LLM Database Update Operation - OpenAI		This strike sends a prompt to manipulate the OpenAI LLM into generating a database-level UPDATE operation. The request is designed to trigger the LLM into producing a SQL query that performs data modification tasks, such as updating existing records in a database. The LLM's response includes a full SQL UPDATE statement which, if executed, could result in unauthorized data changes or corruption of existing information. Target LLM: OpenAI

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike AI LLM Prompt Injection Deceptive Delight - Gemini		This strike sends a "Deceptive Delight" prompt to the Gemini LLM. This technique manipulates the Gemini LLM by embedding harmful prompts that lead the model to generate harmful responses under the guise of providing helpful information. The structured prompt subtly guides the LLM into formulating high-risk responses while appearing innocuous. Note: This strike will randomly select a harmful prompt from the Forbidden questions set and embed it within the prompt. Target LLM: Gemini
Strike AI LLM Prompt Injection Deceptive Delight - Grok		This strike sends a "Deceptive Delight" prompt to the Grok LLM. This technique manipulates the Grok LLM by embedding harmful prompts that lead the model to generate harmful responses under the guise of providing helpful information. The structured prompt subtly guides the LLM into formulating high-risk responses while appearing innocuous. Note: This strike will randomly select a harmful prompt from the Forbidden questions set and embed it within the prompt. Target LLM: Grok
Strike AI LLM Prompt Injection Deceptive Delight - OpenAI		This strike sends a "Deceptive Delight" prompt to the OpenAI LLM. This technique manipulates the OpenAI LLM by embedding harmful prompts that lead the model to generate harmful responses under the guise of providing helpful information. The structured prompt subtly guides the LLM into formulating high-risk responses while appearing innocuous. Note: This strike will randomly select a harmful prompt from the Forbidden questions set and embed it within the prompt. Target LLM: OpenAI
Strike AI LLM Disease Vector URL Prompt - Gemini		This strike sends a disease vector (spyware/grayware, password-cracking applications, key-stroke trackers and virus/malware kit downloads) related URL-based prompt to the Gemini LLM, asking it to generate a response after visiting and analyzing the URL. The request randomly selects such URLs from the dataset and uses them inside the prompt. Target LLM: Gemini
Strike AI LLM Disease Vector URL Prompt - Grok		This strike sends a disease vector (spyware/grayware, password-cracking applications, key-stroke trackers and virus/malware kit downloads) related URL-based prompt to the Grok LLM, asking it to generate a response after visiting and analyzing the URL. The request randomly selects such URLs from the dataset and uses them inside the prompt. Target LLM: Grok
Strike AI LLM Disease Vector URL Prompt - OpenAI		This strike sends a disease vector (spyware/grayware, password-cracking applications, key-stroke trackers and virus/malware kit downloads) related URL-based prompt to the OpenAI LLM, asking it to generate a response after visiting and analyzing the URL. The request randomly selects such URLs from the dataset and uses them inside the prompt. Target LLM: OpenAI
Strike AI LLM Disease Vector URL Response - Gemini		This strike sends a prompt to the Gemini LLM asking it to generate a response which includes disease vector (spyware/grayware, password-cracking applications, key-stroke trackers and virus/malware kit downloads) related URLs. This randomly selects a few URLs from the dataset and uses them inside the LLM response. Target LLM: Gemini

Name	References	Description
Strike AI LLM Disease Vector URL Response - Grok		This strike sends a prompt to the Grok LLM asking it to generate a response which includes disease vector (spyware/grayware, password-cracking applications, key-stroke trackers and virus/malware kit downloads) related URLs. This randomly selects a few URLs from the dataset and uses them inside the LLM response. Target LLM: Grok
Strike AI LLM Disease Vector URL Response - OpenAI		This strike sends a prompt to the OpenAI LLM asking it to generate a response which includes disease vector (spyware/grayware, password-cracking applications, key-stroke trackers and virus/malware kit downloads) related URLs. This randomly selects a few URLs from the dataset and uses them inside the LLM response. Target LLM: OpenAI
Strike AI LLM Link Trap PII Leakage Banking Information - Gemini		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to banking data, such as account holder name, account number, bank balance, registered phone number and email address. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Gemini
Strike AI LLM Link Trap PII Leakage Banking Information - Grok		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to banking data, such as account holder name, account number, bank balance, registered phone number and email address. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Grok

Name	References	Description
Strike AI LLM Link Trap PII Leakage Banking Information - OpenAI		<p>This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to banking data, such as account holder name, account number, bank balance, registered phone number and email address. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: OpenAI</p>
Strike AI LLM Link Trap PII Leakage Biometric Data - Gemini		<p>This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to biometric data. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Gemini</p>
Strike AI LLM Link Trap PII Leakage Biometric Data - Grok		<p>This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to biometric data. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Grok</p>

Name	References	Description
Strike AI LLM Link Trap PII Leakage Biometric Data - OpenAI		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to biometric data. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: OpenAI
Strike AI LLM Link Trap PII Leakage Customer Support Information - Gemini		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to customer support interactions, such as customer name, email address, phone number and home address. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Gemini
Strike AI LLM Link Trap PII Leakage Customer Support Information - Grok		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to customer support interactions, such as customer name, email address, phone number and home address. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Grok

Name	References	Description
Strike AI LLM Link Trap PII Leakage Customer Support Information - OpenAI		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to customer support interactions, such as customer name, email address, phone number and home address. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: OpenAI
Strike AI LLM Link Trap PII Leakage Employee Record - Gemini		This strike sends a multi-turn prompt to the LLM, including a PII-containing prompt, a static greeting, a safe query, and a request for a base64-encoded link. It tests the LLM's ability to handle sensitive data and generate safe responses. PII and safe prompts are randomized from pseudo-playlists. Target LLM: Gemini
Strike AI LLM Link Trap PII Leakage Employee Record - Grok		This strike sends a multi-turn prompt to the LLM, including a PII-containing prompt, a static greeting, a safe query, and a request for a base64-encoded link. It tests the LLM's ability to handle sensitive data and generate safe responses. PII and safe prompts are randomized from pseudo-playlists. Target LLM: Grok
Strike AI LLM Link Trap PII Leakage Employee Record - OpenAI		This strike sends a multi-turn prompt to the LLM, including a PII-containing prompt, a static greeting, a safe query, and a request for a base64-encoded link. It tests the LLM's ability to handle sensitive data and generate safe responses. PII and safe prompts are randomized from pseudo-playlists. Target LLM: OpenAI
Strike AI LLM Link Trap PII Leakage Government Document - Gemini		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to government records, such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Gemini

Name	References	Description
Strike AI LLM Link Trap PII Leakage Government Document - Grok		<p>This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to government records, such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM.</p> <p>Target LLM: Grok</p>
Strike AI LLM Link Trap PII Leakage Government Document - OpenAI		<p>This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to government records, such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM.</p> <p>Target LLM: OpenAI</p>
Strike AI LLM Link Trap PII Leakage PHI Disclosure - Gemini		<p>This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to Protected Health Information (PHI), such as patient name, medical record number, hospital name, insurance number, physician name, contact details, admission date and discharge date. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM.</p> <p>Target LLM: Gemini</p>

Name	References	Description
Strike AI LLM Link Trap PII Leakage PHI Disclosure - Grok		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to Protected Health Information (PHI), such as patient name, medical record number, hospital name, insurance number, physician name, contact details, admission date and discharge date. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Grok
Strike AI LLM Link Trap PII Leakage PHI Disclosure - OpenAI		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to Protected Health Information (PHI), such as patient name, medical record number, hospital name, insurance number, physician name, contact details, admission date and discharge date. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: OpenAI
Strike AI LLM Malware URL Prompt - Gemini		This strike sends a malware URL-based prompt to the Gemini LLM, asking it to generate a response after visiting and analyzing the URL. The request randomly selects a few malware related URLs from the dataset and uses them inside the prompt. Target LLM: Gemini
Strike AI LLM Malware URL Prompt - Grok		This strike sends a malware URL-based prompt to the Grok LLM, asking it to generate a response after visiting and analyzing the URL. The request randomly selects a few malware related URLs from the dataset and uses them inside the prompt. Target LLM: Grok
Strike AI LLM Malware URL Prompt - OpenAI		This strike sends a malware URL-based prompt to the OpenAI LLM, asking it to generate a response after visiting and analyzing the URL. The request randomly selects a few malware related URLs from the dataset and uses them inside the prompt. Target LLM: OpenAI
Strike AI LLM Malware URL Response - Gemini		This strike sends a prompt to the Gemini LLM asking it to generate a response which includes malware URLs. This randomly selects a few malware related URLs from the dataset and uses them inside the LLM response. Target LLM: Gemini

Name	References	Description
Strike AI LLM Malware URL Response - Grok		This strike sends a prompt to the Grok LLM asking it to generate a response which includes malware URLs. This randomly selects a few malware related URLs from the dataset and uses them inside the LLM response. Target LLM: Grok
Strike AI LLM Malware URL Response - OpenAI		This strike sends a prompt to the OpenAI LLM asking it to generate a response which includes malware URLs. This randomly selects a few malware related URLs from the dataset and uses them inside the LLM response. Target LLM: OpenAI
Strike AI LLM Phishing URL Prompt - Gemini		This strike sends a phishing URL-based prompt to the Gemini LLM, asking it to generate a response after analyzing the URL or crafting phishing content. The request randomly selects a few phishing related URLs from the dataset and uses them inside the prompt. Target LLM: Gemini
Strike AI LLM Phishing URL Prompt - Grok		This strike sends a phishing URL-based prompt to the Grok LLM, asking it to generate a response after analyzing the URL or crafting phishing content. The request randomly selects a few phishing related URLs from the dataset and uses them inside the prompt. Target LLM: Grok
Strike AI LLM Phishing URL Prompt - OpenAI		This strike sends a phishing URL-based prompt to the OpenAI LLM, asking it to generate a response after analyzing the URL or crafting phishing content. The request randomly selects a few phishing related URLs from the dataset and uses them inside the prompt. Target LLM: OpenAI
Strike AI LLM Phishing URL Response - Gemini		This strike sends a prompt to the Gemini LLM asking it to generate a response which includes phishing URLs. This randomly selects a few phishing related URLs from the dataset and uses them inside the LLM response. Target LLM: Gemini
Strike AI LLM Phishing URL Response - Grok		This strike sends a prompt to the Grok LLM asking it to generate a response which includes phishing URLs. This randomly selects a few phishing related URLs from the dataset and uses them inside the LLM response. Target LLM: Grok
Strike AI LLM Phishing URL Response - OpenAI		This strike sends a prompt to the OpenAI LLM asking it to generate a response which includes phishing URLs. This randomly selects a few phishing related URLs from the dataset and uses them inside the LLM response. Target LLM: OpenAI
Strike AI LLM PII in User Requests Banking Information Disclosure - Gemini		This strike involves crafting a user request that contains personally identifiable information (PII) related to banking. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as account number, card number, CVV, expiration date, net banking credentials, or personal identification numbers. Target LLM: Gemini

Name	References	Description
Strike AI LLM PII in User Requests Banking Information Disclosure - Grok		This strike involves crafting a user request that contains personally identifiable information (PII) related to banking. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as account number, card number, CVV, expiration date, net banking credentials, or personal identification numbers. Target LLM: Grok
Strike AI LLM PII in User Requests Banking Information Disclosure - OpenAI		This strike involves crafting a user request that contains personally identifiable information (PII) related to banking. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as account number, card number, CVV, expiration date, net banking credentials, or personal identification numbers. Target LLM: OpenAI
Strike AI LLM PII in User Requests Biometric Data Disclosure - Gemini		This strike involves crafting a user request that contains personally identifiable information (PII) related to biometric data. The simulated request mimics real-world user behavior, where individuals might inadvertently disclose sensitive details such as fingerprint enrollment status, facial recognition setup information, voice authentication data, iris scan IDs, palm scan IDs, along with associated identifiers like employee ID, passport number, and date of birth. Target LLM: Gemini
Strike AI LLM PII in User Requests Biometric Data Disclosure - Grok		This strike involves crafting a user request that contains personally identifiable information (PII) related to biometric data. The simulated request mimics real-world user behavior, where individuals might inadvertently disclose sensitive details such as fingerprint enrollment status, facial recognition setup information, voice authentication data, iris scan IDs, palm scan IDs, along with associated identifiers like employee ID, passport number, and date of birth. Target LLM: Grok
Strike AI LLM PII in User Requests Biometric Data Disclosure - OpenAI		This strike involves crafting a user request that contains personally identifiable information (PII) related to biometric data. The simulated request mimics real-world user behavior, where individuals might inadvertently disclose sensitive details such as fingerprint enrollment status, facial recognition setup information, voice authentication data, iris scan IDs, palm scan IDs, along with associated identifiers like employee ID, passport number, and date of birth. Target LLM: OpenAI
Strike AI LLM PII in User Requests Customer Support Data Disclosure - Gemini		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: Gemini
Strike AI LLM PII in User Requests Customer Support Data Disclosure - Grok		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: Grok

Name	References	Description
Strike AI LLM PII in User Requests Customer Support Data Disclosure - OpenAI		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: OpenAI
Strike AI LLM PII in User Requests Employee Record Disclosure - Gemini		This strike involves crafting a user request that contains personally identifiable information (PII) related to employee records. The simulated request mimics real-world user behavior, where individuals might inadvertently share confidential details such as employee name, company name, job title, employee ID, email address, contact number, and home address. Target LLM: Gemini
Strike AI LLM PII in User Requests Employee Record Disclosure - Grok		This strike involves crafting a user request that contains personally identifiable information (PII) related to employee records. The simulated request mimics real-world user behavior, where individuals might inadvertently share confidential details such as employee name, company name, job title, employee ID, email address, contact number, and home address. Target LLM: Grok
Strike AI LLM PII in User Requests Employee Record Disclosure - OpenAI		This strike involves crafting a user request that contains personally identifiable information (PII) related to employee records. The simulated request mimics real-world user behavior, where individuals might inadvertently share confidential details such as employee name, company name, job title, employee ID, email address, contact number, and home address. Target LLM: OpenAI
Strike AI LLM PII in User Requests Government Document Disclosure - Gemini		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: Gemini
Strike AI LLM PII in User Requests Government Document Disclosure - Grok		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: Grok
Strike AI LLM PII in User Requests Government Document Disclosure - OpenAI		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: OpenAI
Strike AI LLM PII in User Requests Protected Health Information (PHI) Disclosure - Gemini		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: Gemini

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike AI LLM PII in User Requests Protected Health Information (PHI) Disclosure - Grok		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: Grok
Strike AI LLM PII in User Requests Protected Health Information (PHI) Disclosure - OpenAI		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: OpenAI
Strike AI LLM Prompt Injection Adaptive Attack Claude template - Gemini		This strike sends a AdaptiveAttack based jailbreak prompt type to the Gemini LLM. This attack sends refined-best-simple prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Gemini
Strike AI LLM Prompt Injection Adaptive Attack Claude template - Grok		This strike sends a AdaptiveAttack based jailbreak prompt type to the Grok LLM. This attack sends refined-best-simple prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Grok
Strike AI LLM Prompt Injection Adaptive Attack Claude template - OpenAI		This strike sends a AdaptiveAttack based jailbreak prompt type to the OpenAI LLM. This attack sends refined-best-simple prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: OpenAI
Strike AI LLM Prompt Injection Adaptive Attack ICL One Shot template - Gemini		This strike sends a AdaptiveAttack based jailbreak prompt type to the Gemini LLM. This attack sends icl-one-shot prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour Target LLM: Gemini
Strike AI LLM Prompt Injection Adaptive Attack ICL One Shot template - Grok		This strike sends a AdaptiveAttack based jailbreak prompt type to the Grok LLM. This attack sends icl-one-shot prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour Target LLM: Grok

Name	References	Description
Strike AI LLM Prompt Injection Adaptive Attack ICL One Shot template - OpenAI		This strike sends a AdaptiveAttack based jailbreak prompt type to the OpenAI LLM. This attack sends icl-one-shot prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour Target LLM: OpenAI
Strike AI LLM Prompt Injection Adaptive Attack Refined Best Simple template - Gemini		This strike sends a AdaptiveAttack based jailbreak prompt type to the Gemini LLM. This attack sends refined-best-simple prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Gemini
Strike AI LLM Prompt Injection Adaptive Attack Refined Best Simple template - Grok		This strike sends a AdaptiveAttack based jailbreak prompt type to the Grok LLM. This attack sends refined-best-simple prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Grok
Strike AI LLM Prompt Injection Adaptive Attack Refined Best Simple template - OpenAI		This strike sends a AdaptiveAttack based jailbreak prompt type to the OpenAI LLM. This attack sends refined-best-simple prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: OpenAI
Strike AI LLM Prompt Injection Adaptive Attack Refined Simple template - Gemini		This strike sends a AdaptiveAttack based jailbreak prompt type to the Gemini LLM. This attack sends refined-best prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Gemini
Strike AI LLM Prompt Injection Adaptive Attack Refined Simple template - Grok		This strike sends a AdaptiveAttack based jailbreak prompt type to the Grok LLM. This attack sends refined-best prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Grok
Strike AI LLM Prompt Injection Adaptive Attack Refined Simple template - OpenAI		This strike sends a AdaptiveAttack based jailbreak prompt type to the OpenAI LLM. This attack sends refined-best prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: OpenAI

Name	References	Description
Strike AI LLM Prompt Injection P2SQL - Gemini		This strike sends a prompt to manipulate the Gemini LLM into generating a database-level CRUD (Create, Read, Update, Delete) operation. The request is designed to trigger the LLM into producing a SQL query that performs data manipulation tasks, such as creating new records, reading existing data, updating records, or deleting entries. The LLM's response includes a full SQL statement which, if executed, could result in unauthorized database changes or exposure of sensitive information. Target LLM: Gemini
Strike AI LLM Prompt Injection P2SQL - Grok		This strike sends a prompt to manipulate the Grok LLM into generating a database-level CRUD (Create, Read, Update, Delete) operation. The request is designed to trigger the LLM into producing a SQL query that performs data manipulation tasks, such as creating new records, reading existing data, updating records, or deleting entries. The LLM's response includes a full SQL statement which, if executed, could result in unauthorized database changes or exposure of sensitive information. Target LLM: Grok
Strike AI LLM Prompt Injection P2SQL - OpenAI		This strike sends a prompt to manipulate the OpenAI LLM into generating a database-level CRUD (Create, Read, Update, Delete) operation. The request is designed to trigger the LLM into producing a SQL query that performs data manipulation tasks, such as creating new records, reading existing data, updating records, or deleting entries. The LLM's response includes a full SQL statement which, if executed, could result in unauthorized database changes or exposure of sensitive information. Target LLM: OpenAI

## New Malware Samples (388)

Attack profile that aims to simulate malwares.

Name	Description
Strike Allakore_058bde7b	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 058bde7b3385b70d59120b24390377af.
Strike Allakore_09096930	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 09096930751d28d388d3e0de003bcb7b.
Strike Allakore_12dbbfcc	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 12dbbfcccd463ec884f788abd5933f8aa.
Strike Allakore_237a12a9	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 237a12a9d67614edd079c02f0f24ed45.
Strike Allakore_29a9d202	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 29a9d202ba2d46047edba9539abba0cd.
Strike Allakore_2f0b96c3	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 2f0b96c3262108012dcf9a940ae461da.
Strike Allakore_32d491d6	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 32d491d6b036c6349c4d2c3bf44011d8.
Strike Allakore_35932f58	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 35932f5856dbf8ba51e048b3b2bb2d7b.

<b>Name</b>	<b>Description</b>
Strike Allakore_3bed8895	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 3bed8895828ba27761b62e9c4ebcc2db.
Strike Allakore_40291ec2	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 40291ec2bd7f23aa76435d5d14f96758.
Strike Allakore_42300099	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 42300099a726353abfdbfd5773de83.
Strike Allakore_47ead282	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 47ead282cd7c6a667d9b4cc9b0c6935e.
Strike Allakore_59401f25	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 59401f25ac88f1c1fe0a5981dc29ea57.
Strike Allakore_59c6ae6b	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 59c6ae6bbe3d048d267d4900c9585828.
Strike Allakore_733f33fa	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 733f33faedb263d914163043b5242f0a.
Strike Allakore_746c9f8f	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 746c9f8f002fb8569d19cb2cdc1295ed.
Strike Allakore_750a3353	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 750a33531763724e8db051750a08cf99.

<b>Name</b>	<b>Description</b>
Strike Allakore_768a78b4	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 768a78b4b12efe721139c474fbf139f4.
Strike Allakore_80151f17	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 80151f17cd04b05f7765071c40215c40.
Strike Allakore_81444a9c	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 81444a9c9f74be2c8ba32542bcc68bab.
Strike Allakore_a3d03ec0	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is a3d03ec08345e7cf02818122fc5b31f3.
Strike Allakore_a50d0d1b	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is a50d0d1bf9ab8291e986e59ebd92be14.
Strike Allakore_aa8b32b2	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is aa8b32b21dcf44a332f9c9d13af3cd7d.
Strike Allakore_ac69851a	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is ac69851a5144e0eb28923ca2e3b8cbe2.
Strike Allakore_b2cb036f	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is b2cb036f919d3cd003023c95c4bbb983.
Strike Allakore_b90a102f	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is b90a102fccedad57b06dc8fb6a58895b.

<b>Name</b>	<b>Description</b>
Strike Allakore_b99d788c	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is b99d788c4dcfd8cc7140e840bd8f5095.
Strike Allakore_bd378258	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is bd3782580c0ddbda2288b2d5d5a72258.
Strike Allakore_bd9d9a4b	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is bd9d9a4be3d93acf3228607b435a4828.
Strike Allakore_c48f0372	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is c48f0372aecf3a7c3d8fab599e7afcde.
Strike Allakore_c74e97cf	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is c74e97cf0086782ab8d22919b11f9c9d.
Strike Allakore_d355ff7b	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is d355ff7b4e022eff5c2b5a5aabae5ad0.
Strike Allakore_d72dfe82	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is d72dfe82b6072cb349120abdbd383aca.
Strike Allakore_df9b2ff8	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is df9b2ff8bd9164ae0f2c802c555d2c4f.
Strike Allakore_e6416904	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is e641690408faf6320fd7c820644ec889.

<b>Name</b>	<b>Description</b>
Strike Allakore_e78fa70b	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is e78fa70b0e38c7c8c29048ceba2dd74.
Strike AsyncRAT_07f3f073	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 07f3f073391f7308ca1c7ef54d6c5656.
Strike AsyncRAT_0a82a328	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 0a82a32801a0a2c1bcf4371a4a582f5e.
Strike AsyncRAT_55a0c7d6	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 55a0c7d6356dfa4c7b45ef03caf2ac75.
Strike AsyncRAT_5b02fac6	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 5b02fac6ed22c683e36715e3c7ae05fc.

<b>Name</b>	<b>Description</b>
Strike AsyncRAT_5ee0d653	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 5ee0d653dba5a4308a7bf5da642daff1.
Strike AsyncRAT_67fefa4b	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 67fefa4bc5ee224e814bea6602399df8.
Strike AsyncRAT_73bd7a8e	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 73bd7a8efb5d7150633432bde16cd980.
Strike AsyncRAT_825a5d12	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 825a5d120ab305b5e12731307a0bee63.
Strike AsyncRAT_8d019622	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 8d01962215ddfe754b725fa9f835b2d6.

<b>Name</b>	<b>Description</b>
Strike AsyncRAT_94719304	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 94719304694a573b087d7efdd8ab8eed.
Strike AsyncRAT_9b1b21fe	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 9b1b21fe9b8ab2fb386dd5794c272baf.
Strike AsyncRAT_b29edf77	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is b29edf77f9af40aaaf7e5387f722d4e32.
Strike AsyncRAT_b4323259	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is b4323259d83bf99fd6f029a3c0d7e272.
Strike AsyncRAT_c2ce2c2a	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is c2ce2c2acb3b2f2ac33f459b850ba40d.

<b>Name</b>	<b>Description</b>
Strike AsyncRAT_c68996a7	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is c68996a7db8547fcbf2f3fd82a5e80ca.
Strike AsyncRAT_d4abb12d	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is d4abb12d79d42b0f392451c49cbe6733.
Strike BQTLock_058a1dbf	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is 058a1dbfa03cac6cc67d34a4dcc69445.
Strike BQTLock_110df495	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is 110df49522d46b612a28bafbdff3405c.
Strike BQTLock_3478194a	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is 3478194a509ae4d2f0a31435952b27bc.

<b>Name</b>	<b>Description</b>
Strike BQTLock_69e6fa25	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is 69e6fa25e66c23121826805bbcb890ac.
Strike BQTLock_84c7bf0	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is 84c7bf0e243dd99b674e48701acob6b.
Strike BQTLock_9569c863	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is 9569c8631bcd37da1a5048d979362804.
Strike BQTLock_972b1677	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is 972b1677621bbdc45ef61c56cd9909d2.
Strike BQTLock_a441e0a2	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is a441e0a25276952bb4fa2f29e06fc209.
Strike BQTLock_a6d91094	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is a6d91094a222da6576260abf52a07b79.

<b>Name</b>	<b>Description</b>
Strike BQTLock_acf3b7f2	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is acf3b7f2f07f5d04083f99b82eb0c8ba.
Strike BQTLock_b098f677	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is b098f67726a4a3f7277b3f41a86d503c.
Strike BQTLock_bc8cc3ca	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is bc8cc3ca2a45ebb934cd71218d9b56b3.
Strike BQTLock_c34d690b	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is c34d690bbe1f9dc78066c881e3596505.
Strike BQTLock_d6476590	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is d647659069d09b59a0e5d3608df314b2.
Strike BQTLock_d6cb9f18	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is d6cb9f18705c34c515dbfd59c4015576.

Name	Description
Strike BQTLock_dae6729c	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is dae6729cc3bfcbd700fc7e46818aada2.
Strike BQTLock_e73abc48	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is e73abc48015c54214b2edae4a6d1ed25.
Strike BlockBlaster_2b366e71	This strike sends a malware sample known as BlockBlaster. BlockBlaster is a malware that is delivered through the game "Abstractism" available on Steam. The malware is delivered via a game update which disguises it as an item drop system. Upon execution, the malware uses the victim's hardware to mine cryptocurrency, slowing down the system performance. Key capabilities of this malware include evasion techniques, cryptocurrency mining, and potentially stealing Steam credentials. The MD5 hash of this BlockBlaster sample is 2b366e711484cb6648e02bc9d7774f3f.
Strike BlockBlaster_7aa6b31c	This strike sends a malware sample known as BlockBlaster. BlockBlaster is a malware that is delivered through the game "Abstractism" available on Steam. The malware is delivered via a game update which disguises it as an item drop system. Upon execution, the malware uses the victim's hardware to mine cryptocurrency, slowing down the system performance. Key capabilities of this malware include evasion techniques, cryptocurrency mining, and potentially stealing Steam credentials. The MD5 hash of this BlockBlaster sample is 7aa6b31c1531f57d744dc7fde5e92338.
Strike BlockBlaster_a80a3dc3	This strike sends a malware sample known as BlockBlaster. BlockBlaster is a malware that is delivered through the game "Abstractism" available on Steam. The malware is delivered via a game update which disguises it as an item drop system. Upon execution, the malware uses the victim's hardware to mine cryptocurrency, slowing down the system performance. Key capabilities of this malware include evasion techniques, cryptocurrency mining, and potentially stealing Steam credentials. The MD5 hash of this BlockBlaster sample is a80a3dc310429fd2d98228e49157f35a.
Strike BlockBlaster_d35249a3	This strike sends a malware sample known as BlockBlaster. BlockBlaster is a malware that is delivered through the game "Abstractism" available on Steam. The malware is delivered via a game update which disguises it as an item drop system. Upon execution, the malware uses the victim's hardware to mine cryptocurrency, slowing down the system performance. Key capabilities of this malware include evasion techniques, cryptocurrency mining, and potentially stealing Steam credentials. The MD5 hash of this BlockBlaster sample is d35249a3f80fdbd17f2664e3408f78e9.

<b>Name</b>	<b>Description</b>
Strike BlockBlaster_dd8da7ba	This strike sends a malware sample known as BlockBlaster. BlockBlaster is a malware that is delivered through the game "Abstractism" available on Steam. The malware is delivered via a game update which disguises it as an item drop system. Upon execution, the malware uses the victim's hardware to mine cryptocurrency, slowing down the system performance. Key capabilities of this malware include evasion techniques, cryptocurrency mining, and potentially stealing Steam credentials. The MD5 hash of this BlockBlaster sample is dd8da7bae76527590f171eeda5a41987.
Strike BlockBlaster_f240341a	This strike sends a malware sample known as BlockBlaster. BlockBlaster is a malware that is delivered through the game "Abstractism" available on Steam. The malware is delivered via a game update which disguises it as an item drop system. Upon execution, the malware uses the victim's hardware to mine cryptocurrency, slowing down the system performance. Key capabilities of this malware include evasion techniques, cryptocurrency mining, and potentially stealing Steam credentials. The MD5 hash of this BlockBlaster sample is f240341a95f7df4c154520b841d1a5e3.
Strike CastleRAT_14610b22	This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is 14610b22a749a0cd464d1985abbff45f.
Strike CastleRAT_22b5bf29	This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is 22b5bf2931140fae49228ced1d1dd3d7.
Strike CastleRAT_35f81d06	This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is 35f81d066028f5e69508956bed79d3ee.

<b>Name</b>	<b>Description</b>
Strike CastleRAT_669fce84	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is 669fce84d112e62291e96f49d42be557.</p>
Strike CastleRAT_9e21fbc9	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is 9e21fbc9e7862fb0d8ba59cf0f16037c.</p>
Strike CastleRAT_a0e6555a	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is a0e6555acf7d7a273b76067f89884705.</p>
Strike CastleRAT_ac77ab1a	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is ac77ab1a3f5a3691e23265bc495e84e8.</p>
Strike CastleRAT_bd61d42f	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is bd61d42f552a7288cfb474498f2f43fc.</p>

<b>Name</b>	<b>Description</b>
Strike CastleRAT_c7fed6e5	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is c7fed6e5ad87ab5c13163300f2dfa500.</p>
Strike CastleRAT_ce7e6656	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is ce7e6656eb256a8b750097ff8e90ade5.</p>
Strike CastleRAT_d195e390	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is d195e39044641f3b1f74843318bca182.</p>
Strike CastleRAT_f1ecdad8	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is f1ecdad8fda4bdaa29fbda8f946a8e47.</p>
Strike CastleRAT_f6ebab2c	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is f6ebab2c29256aaca8f8b8b6da89e6eb.</p>

<b>Name</b>	<b>Description</b>
Strike ClayRAT_0658b719	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 0658b719a2dcb7762743af4ea97646af.
Strike ClayRAT_074b5622	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 074b5622421e8ed778af7d0c013c365c.
Strike ClayRAT_0abb2947	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 0abb29472275a0d558839e3fb16a2407.
Strike ClayRAT_198505a6	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 198505a6ac0ff95b4f9cada0a7f7a393.
Strike ClayRAT_49e0f3d2	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 49e0f3d2284ed076ad5a72af97548fba.
Strike ClayRAT_57149137	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 57149137ee7145ad106cdac344e70c85.

<b>Name</b>	<b>Description</b>
Strike ClayRAT_5a0f7c94	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 5a0f7c94841306c309da7dc3045071e5.
Strike ClayRAT_698fd171	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 698fd1710d7fae4308022bf181d62b4d.
Strike ClayRAT_7c87ffd8	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 7c87ffd8dfd36ceedcf0e2a45f059c0b.
Strike ClayRAT_91a10457	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 91a10457b782945178c5c6a2f4c60123.
Strike ClayRAT_9bd27080	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 9bd2708072b016777c412d475b8b6720.
Strike ClayRAT_aa5c7f83	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is aa5c7f832eb47c8b6acaf9fcbe87a699.

<b>Name</b>	<b>Description</b>
Strike ClayRAT_c5b7070e	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is c5b7070ee6e114e2311d200afdb0c804.
Strike ClayRAT_c8200034	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is c82000348c9b5a302bd5073b52c13221.
Strike ClayRAT_e2f3d7bc	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is e2f3d7bcd79bc500a64478977cb50efb.
Strike ClayRAT_e78cdced	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is e78cdced64bc65e392faeed019812a62.
Strike DeceptiveDevelopment_250 443d3	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is 250443d3d3fe43e9d0ecacba69130842.
Strike DeceptiveDevelopment_3ae d5502	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is 3aed5502118eb9b8c9f8a779d4b09e11.

<b>Name</b>	<b>Description</b>
Strike DeceptiveDevelopment_3ef7 717c	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is 3ef7717c8bcb26396fc50ed92e812d13.
Strike DeceptiveDevelopment_535 03cbe	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is 53503cbe1d3f62e4b5fd3245ce144858.
Strike DeceptiveDevelopment_617 5efd1	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is 6175efd148a89ca61b6835c77acc7a8d.
Strike DeceptiveDevelopment_6d7 68860	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is 6d76886042d1d6957fec9b60cb4cc78d.
Strike DeceptiveDevelopment_a00 9cd35	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is a009cd35850929199ef60e71bce86830.

Name	Description
Strike DeceptiveDevelopment_b29 ddcc9	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is b29ddcc9affdd56a520f23a61b670134.
Strike DeceptiveDevelopment_b52 e105b	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is b52e105bd040bda6639e958f7d9e3090.
Strike GayFemBoy_03ac6a68	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 03ac6a687be22b30ec48656235fef107.
Strike GayFemBoy_07025e99	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 07025e9990963038249ff2b771ee5d5c.
Strike GayFemBoy_0b6e8d5d	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 0b6e8d5d68dda316da6125d8f6b6ced3.
Strike GayFemBoy_0e17f987	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 0e17f987efa46626eb5d22d6516b3718.

<b>Name</b>	<b>Description</b>
Strike GayFemBoy_100d33b8	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 100d33b8167c0c7d842f0cd93f01648b.
Strike GayFemBoy_12b4f549	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 12b4f549ae5e131f01b0b1181b06c71e.
Strike GayFemBoy_1e715cf1	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 1e715cf11e649b8e294d7877e9ce033b.
Strike GayFemBoy_1e728e64	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 1e728e6439296e9442db6fbcb488bedc.
Strike GayFemBoy_22e99928	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 22e99928283dd4cf0d8de14511ef752d.
Strike GayFemBoy_28343b78	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 28343b780bf5d8b9e6b7a274418f997f.

<b>Name</b>	<b>Description</b>
Strike GayFemBoy_3246002d	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 3246002d1f2e0506af4d13e6847d3a60.
Strike GayFemBoy_431dbc9e	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 431dbc9e8e1b6cad13f5843fd3ea18b9.
Strike GayFemBoy_4408fca1	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 4408fca1a089360be769be08000fc5a1.
Strike GayFemBoy_513c7b85	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 513c7b85dfa334c0239a6446f88e148c.
Strike GayFemBoy_5e1a6c16	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 5e1a6c16bee32894b4b950d9eac58192.
Strike GayFemBoy_6259fe5c	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 6259fe5c02fb702a85c557627af242.

<b>Name</b>	<b>Description</b>
Strike GayFemBoy_648375d6	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 648375d6acd2e0997a7492f2afbdd878.
Strike GayFemBoy_64f9bb8d	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 64f9bb8df99874eca578f0ce9744aad1.
Strike GayFemBoy_69b85867	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 69b85867eca0e3bd7cafd4e3f192c0a8.
Strike GayFemBoy_6e7d22a1	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 6e7d22a17f5534aea0b45f01a008e745.
Strike GayFemBoy_6fad431b	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 6fad431b9d6b5259127fb1e57d23fb87.
Strike GayFemBoy_96946e70	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 96946e70c541e54f352bad8c3fa24b1a.

<b>Name</b>	<b>Description</b>
Strike GayFemBoy_9b31ff6a	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 9b31ff6a02b18bafec874c51a1d2321a.
Strike GayFemBoy_9d10f85e	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 9d10f85e8aaa077b39742f8a54bd75ab.
Strike GayFemBoy_a0a0503b	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is a0a0503bf342c4f82e1aefbf28224550.
Strike GayFemBoy_a166c743	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is a166c743a0141ee18fa912768b767410.
Strike GayFemBoy_a23acaf1	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is a23acaf15e11a623827b44e30ef8c56d.
Strike GayFemBoy_aedae14b	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is aedae14b13971c2f9cf8963c2e6e6667.

<b>Name</b>	<b>Description</b>
Strike GayFemBoy_b1c2b561	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is b1c2b561dd2eae64d89988438bde2639.
Strike GayFemBoy_b9953c35	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is b9953c35f94b231a5e05f818c978c6e2.
Strike GayFemBoy_bd9aecbf	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is bd9aecbfbe099ec9c62873f794b410c5.
Strike GayFemBoy_caaee37ae	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is caee37aec95686de5a033c6334e51799.
Strike GayFemBoy_d7df605f	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is d7df605f7ca64352f40293edc59b57f2.
Strike GayFemBoy_da734b14	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is da734b14aac135abce426ab603b6fb6.

<b>Name</b>	<b>Description</b>
Strike GayFemBoy_f92e579f	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is f92e579f058de6f19d5c40dff1aeb3b2.
Strike GayFemBoy_ff296fc2	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is ff296fc2d3fc35edcbbeda8aefce75d7.
Strike GhostCall_0af11f61	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 0af11f610da1f691e43173d44643283f.
Strike GhostCall_12439688	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 1243968876262c3ad4250e1371447b23.
Strike GhostCall_5ad40a5f	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 5ad40a5fd18a1b57b69c44bc2963dc6b.
Strike GhostCall_6348b49f	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 6348b49f3499d760797247b94385fda3.

<b>Name</b>	<b>Description</b>
Strike GhostCall_76ace3a6	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 76ace3a6892c25512b17ed42ac2ebd05.
Strike GhostCall_931cec3c	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 931cec3c80c78d233e3602a042a2e71b.
Strike GhostCall_9551b4af	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 9551b4af789b2db563f9452eaf46b6aa.
Strike GhostCall_963f473f	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 963f473f1734d8b3fbb8c9a227c06d07.
Strike GhostCall_c42c7a2e	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is c42c7a2ea1c2f00dddb0cc4c8fb5bcf.
Strike GhostCall_c446682f	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is c446682f33641cff21083ac2ce477dbe.

<b>Name</b>	<b>Description</b>
Strike GhostCall_d8529855	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is d8529855fab4b4aa6c2b34449cb3b9fb.
Strike GhostCall_e33f942c	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is e33f942cf1479ca8530a916868bad954.
Strike GhostCall_e8680d17	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is e8680d17fba6425e4a9bb552fb8db2b1.
Strike HybridPetya_096dd6f0	This strike sends a malware sample known as HybridPetya. HybridPetya is a malware of the ransomware family that encrypts the Master File Table (MFT) of the NTFS file system, rendering the system unusable. It is delivered through a fake resume in a Dropbox link sent via email. Upon execution, it forces a system reboot and displays a fake check disk screen while it encrypts the MFT. Its key capabilities include encrypting the MFT, replacing the Master Boot Record (MBR) with a custom bootloader, and demanding a ransom to decrypt the system. The MD5 hash of this HybridPetya sample is 096dd6f0422ea562956e4eb64c48e311.
Strike HybridPetya_67051905	This strike sends a malware sample known as HybridPetya. HybridPetya is a malware of the ransomware family that encrypts the Master File Table (MFT) of the NTFS file system, rendering the system unusable. It is delivered through a fake resume in a Dropbox link sent via email. Upon execution, it forces a system reboot and displays a fake check disk screen while it encrypts the MFT. Its key capabilities include encrypting the MFT, replacing the Master Boot Record (MBR) with a custom bootloader, and demanding a ransom to decrypt the system. The MD5 hash of this HybridPetya sample is 670519058a309a63ff63bbf573f79916.
Strike HybridPetya_67e8ccae	This strike sends a malware sample known as HybridPetya. HybridPetya is a malware of the ransomware family that encrypts the Master File Table (MFT) of the NTFS file system, rendering the system unusable. It is delivered through a fake resume in a Dropbox link sent via email. Upon execution, it forces a system reboot and displays a fake check disk screen while it encrypts the MFT. Its key capabilities include encrypting the MFT, replacing the Master Boot Record (MBR) with a custom bootloader, and demanding a ransom to decrypt the system. The MD5 hash of this HybridPetya sample is 67e8ccaecdc7983a40fc09d239945c4.

<b>Name</b>	<b>Description</b>
Strike HybridPetya_b1592068	This strike sends a malware sample known as HybridPetya. HybridPetya is a malware of the ransomware family that encrypts the Master File Table (MFT) of the NTFS file system, rendering the system unusable. It is delivered through a fake resume in a Dropbox link sent via email. Upon execution, it forces a system reboot and displays a fake check disk screen while it encrypts the MFT. Its key capabilities include encrypting the MFT, replacing the Master Boot Record (MBR) with a custom bootloader, and demanding a ransom to decrypt the system. The MD5 hash of this HybridPetya sample is b15920685a76992ad8179687b3c0a7c3.
Strike HybridPetya_baba1728	This strike sends a malware sample known as HybridPetya. HybridPetya is a malware of the ransomware family that encrypts the Master File Table (MFT) of the NTFS file system, rendering the system unusable. It is delivered through a fake resume in a Dropbox link sent via email. Upon execution, it forces a system reboot and displays a fake check disk screen while it encrypts the MFT. Its key capabilities include encrypting the MFT, replacing the Master Boot Record (MBR) with a custom bootloader, and demanding a ransom to decrypt the system. The MD5 hash of this HybridPetya sample is baba1728a03c8c05b13b57c909778c0a.
Strike HybridPetya_c6854118	This strike sends a malware sample known as HybridPetya. HybridPetya is a malware of the ransomware family that encrypts the Master File Table (MFT) of the NTFS file system, rendering the system unusable. It is delivered through a fake resume in a Dropbox link sent via email. Upon execution, it forces a system reboot and displays a fake check disk screen while it encrypts the MFT. Its key capabilities include encrypting the MFT, replacing the Master Boot Record (MBR) with a custom bootloader, and demanding a ransom to decrypt the system. The MD5 hash of this HybridPetya sample is c6854118f7e9ea0ec3cbd6163e3e2541.
Strike HybridPetya_e184fe6b	This strike sends a malware sample known as HybridPetya. HybridPetya is a malware of the ransomware family that encrypts the Master File Table (MFT) of the NTFS file system, rendering the system unusable. It is delivered through a fake resume in a Dropbox link sent via email. Upon execution, it forces a system reboot and displays a fake check disk screen while it encrypts the MFT. Its key capabilities include encrypting the MFT, replacing the Master Boot Record (MBR) with a custom bootloader, and demanding a ransom to decrypt the system. The MD5 hash of this HybridPetya sample is e184fe6b3244787a71e1d1d4a152a9b5.
Strike Katz_0710c5fd	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 0710c5fd7d53dece6926b297e343d3f2.
Strike Katz_081f29e7	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 081f29e70ee9fc5c98670eb874871547.
Strike Katz_1f86370a	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 1f86370a6a8f6c2757a9f369efdfd52d.

<b>Name</b>	<b>Description</b>
Strike Katz_2644ca19	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 2644ca19399ceb0826ab0bf63af00577.
Strike Katz_2e93e90d	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 2e93e90db74c9c9a606a5cd8e80fce5e.
Strike Katz_3272a23d	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 3272a23dc07e137402aafcdeb25397d4.
Strike Katz_5249739c	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 5249739c4049a32207828449671f0faa.
Strike Katz_542b3f94	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 542b3f9462113c46ec44b0fe6b0681d1.
Strike Katz_63368017	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 6336801701845edb81946b42876a20ac.
Strike Katz_68379cae	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 68379cae8fcb5fc5c29b831727b53c63.
Strike Katz_6bcae382	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 6bcae3827c4a9015319553188ae52edf.
Strike Katz_73462631	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 73462631872be6fb456063f9a7718d6c.
Strike Katz_829f1399	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 829f139966ebe28189dbe3eca8c7296.

<b>Name</b>	<b>Description</b>
Strike Katz_848a89e1	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 848a89e10ff33aae1b4ecf360a1cb1ce.
Strike Katz_98eb2f36	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 98eb2f36b29ae6ae48640b742c8efd63.
Strike Katz_9dca6162	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 9dca61626ab6343fb5e39ce310b367e8.
Strike Katz_a3727ff6	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is a3727ff64c82935d7697e3fefc6af383.
Strike Katz_baf29279	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is baf292797b6d10fadbd32f4ebcd575587.
Strike Katz_cd1dd021	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is cd1dd021e439fd621fc3410bfb2dfb78.
Strike Katz_d384268b	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is d384268b339c7e5440ee1a7607be3495.
Strike Katz_e5d9896e	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is e5d9896e98ac498a76cf4fa4c13f4d04.
Strike Katz_eff3042e	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is eff3042e5f5483212c90dbc70033ed74.
Strike Katz_f175f4c2	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is f175f4c2d99cc4f35f9aecdfffc3489ed.

<b>Name</b>	<b>Description</b>
Strike Katz_f69bf1ed	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is f69bf1ed39691a1c5cabfbadc2faed6c.
Strike Kimsuky_01d3fc28	This strike sends a malware sample known as Kimsuky. Kimsuky is a malware of the spyware family developed by North Korean groups that targets South Korean think tanks and political entities. It is typically delivered through spear-phishing emails that contain malicious Microsoft Word documents. Once executed, the malware collects information from the infected system and sends it back to the attacker's command-and-control server. The key capabilities of Kimsuky include keystroke logging, capturing screenshots, and stealing documents from the infected system. The MD5 hash of this Kimsuky sample is 01d3fc28e052efaa475727d2b759b51f.
Strike Kimsuky_33d48adb	This strike sends a malware sample known as Kimsuky. Kimsuky is a malware of the spyware family developed by North Korean groups that targets South Korean think tanks and political entities. It is typically delivered through spear-phishing emails that contain malicious Microsoft Word documents. Once executed, the malware collects information from the infected system and sends it back to the attacker's command-and-control server. The key capabilities of Kimsuky include keystroke logging, capturing screenshots, and stealing documents from the infected system. The MD5 hash of this Kimsuky sample is 33d48adb6e36de40185eee6a649274a0.
Strike Kimsuky_349de8d6	This strike sends a malware sample known as Kimsuky. Kimsuky is a malware of the spyware family developed by North Korean groups that targets South Korean think tanks and political entities. It is typically delivered through spear-phishing emails that contain malicious Microsoft Word documents. Once executed, the malware collects information from the infected system and sends it back to the attacker's command-and-control server. The key capabilities of Kimsuky include keystroke logging, capturing screenshots, and stealing documents from the infected system. The MD5 hash of this Kimsuky sample is 349de8d66501b53a38beca5b331d98e5.
Strike Kimsuky_59d11524	This strike sends a malware sample known as Kimsuky. Kimsuky is a malware of the spyware family developed by North Korean groups that targets South Korean think tanks and political entities. It is typically delivered through spear-phishing emails that contain malicious Microsoft Word documents. Once executed, the malware collects information from the infected system and sends it back to the attacker's command-and-control server. The key capabilities of Kimsuky include keystroke logging, capturing screenshots, and stealing documents from the infected system. The MD5 hash of this Kimsuky sample is 59d1152449a503665f552cba0455f02d.
Strike Kimsuky_a8269069	This strike sends a malware sample known as Kimsuky. Kimsuky is a malware of the spyware family developed by North Korean groups that targets South Korean think tanks and political entities. It is typically delivered through spear-phishing emails that contain malicious Microsoft Word documents. Once executed, the malware collects information from the infected system and sends it back to the attacker's command-and-control server. The key capabilities of Kimsuky include keystroke logging, capturing screenshots, and stealing documents from the infected system. The MD5 hash of this Kimsuky sample is a8269069133ecf1924db2b5d712f33ad.

<b>Name</b>	<b>Description</b>
Strike Kimsuky_efee226c	This strike sends a malware sample known as Kimsuky. Kimsuky is a malware of the spyware family developed by North Korean groups that targets South Korean think tanks and political entities. It is typically delivered through spear-phishing emails that contain malicious Microsoft Word documents. Once executed, the malware collects information from the infected system and sends it back to the attacker's command-and-control server. The key capabilities of Kimsuky include keystroke logging, capturing screenshots, and stealing documents from the infected system. The MD5 hash of this Kimsuky sample is efee226c8dc22cc3090709202b853970.
Strike Klopatra_26e59fbf	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is 26e59fbfa6bedc8910638c44986cf8f4.
Strike Klopatra_34ced080	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is 34ced080497311f03e7e5e8ef01b0db3.
Strike Klopatra_4ef93b8b	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is 4ef93b8bb360b87958b8e1f70c0438b8.
Strike Klopatra_7d55b181	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is 7d55b1815aae99cab061fbfd1908e87.

<b>Name</b>	<b>Description</b>
Strike Klopatra_7eb52c6f	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is 7eb52c6f4fd646190b2ba518226a4cdd.
Strike Klopatra_7fe5950a	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is 7fe5950ad2772ac64363e952022a49a5.
Strike Klopatra_ac55f4e3	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is ac55f4e37bb097892100ea25f6dae3cf.
Strike Klopatra_b5988fbc	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is b5988fbce2365e62803a613508070780.
Strike Klopatra_ce73486e	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is ce73486ef665a71f882489e68f842a40.

<b>Name</b>	<b>Description</b>
Strike Klopatra_d553a2db	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is d553a2dbd3076c45008ce4009dff8b97.
Strike Klopatra_d606d84e	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is d606d84eff5f24502204ef5a86af0319.
Strike Klopatra_f8e6ce9e	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is f8e6ce9e7d1749c8f7712ff7c5e16b62.
Strike Klopatra_fa1d6028	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is fa1d6028d68b1d117438915edcb178f8.
Strike LunarSpider_21cde10c	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 21cde10c7da48bab622e75d6004d61de.

<b>Name</b>	<b>Description</b>
Strike LunarSpider_2a743bcc	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 2a743bcc9cee1900a0457127abeade60.
Strike LunarSpider_2c3d09cd	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 2c3d09cd1d8aea8cc7049296782c8def.
Strike LunarSpider_330a6bae	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 330a6bae00ad4be4a0df732520905395.
Strike LunarSpider_33f6c6b3	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 33f6c6b3727a233819111e3b3aae96ec.
Strike LunarSpider_3f21939c	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 3f21939c7db0c894b74c361d72d044db.

<b>Name</b>	<b>Description</b>
Strike LunarSpider_56d21ac3	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 56d21ac3631f52b18325224214dcbd73.
Strike LunarSpider_628d88e9	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 628d88e98c44d9846954fd7bbb8e143.
Strike LunarSpider_66b559df	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 66b559df3b20b0280322e9bf67752d6a.
Strike LunarSpider_97be7a2e	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 97be7a2e8918be589396de0eaf97a590.
Strike LunarSpider_a0ffaf70	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is a0ffaf708b8c44e7fd3a5a505acc015b.

<b>Name</b>	<b>Description</b>
Strike LunarSpider_a3254b2e	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is a3254b2ef6bca343aa158261d7a46c50.
Strike LunarSpider_d58be0d4	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is d58be0d4dcc144ca9d6a1ecf9e8232f9.
Strike LunarSpider_e0df61c7	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is e0df61c7e5c764396970dd47d4589c01.
Strike LunarSpider_fd817202	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is fd817202314d4067c2dc9c51d98f0268.
Strike Maranhao_bf646eec	This strike sends a malware sample known as Maranhao. Maranhao Stealer is a Node.js powered malware of the info-stealer type that targets sensitive user data. It is delivered through phishing emails containing malicious attachments or links. Upon execution, it collects various types of sensitive information including browser data, cryptocurrency wallets, and system information. Its key capabilities include data exfiltration, system information collection, and credential theft from multiple sources such as browsers and cryptocurrency wallets. The MD5 hash of this Maranhao sample is bf646eec3161c66a48001eba3e2772a4.

Name	Description
Strike Maranhao_c9912bd4	This strike sends a malware sample known as Maranhao. Maranhao Stealer is a Node.js powered malware of the info-stealer type that targets sensitive user data. It is delivered through phishing emails containing malicious attachments or links. Upon execution, it collects various types of sensitive information including browser data, cryptocurrency wallets, and system information. Its key capabilities include data exfiltration, system information collection, and credential theft from multiple sources such as browsers and cryptocurrency wallets. The MD5 hash of this Maranhao sample is c9912bd4cb21fa0fc9fc1a0311cb95ed.
Strike Maranhao_dc2ebe2f	This strike sends a malware sample known as Maranhao. Maranhao Stealer is a Node.js powered malware of the info-stealer type that targets sensitive user data. It is delivered through phishing emails containing malicious attachments or links. Upon execution, it collects various types of sensitive information including browser data, cryptocurrency wallets, and system information. Its key capabilities include data exfiltration, system information collection, and credential theft from multiple sources such as browsers and cryptocurrency wallets. The MD5 hash of this Maranhao sample is dc2ebe2fb7935f7b2161dd4eb93d961d.
Strike PhantomNet_0fbc2bf2	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 0fbc2bf2f66fc72c521a9b8561bab1da.
Strike PhantomNet_1498f1df	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 1498f1df4ca0e9cf23babe00cf34ed3d.
Strike PhantomNet_2632fa8f	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 2632fa8fc67dd2fd5c5a6275465dcc95.

<b>Name</b>	<b>Description</b>
Strike PhantomNet_3b4ea607	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 3b4ea6079ac9f154e0d4ec2cb6d05431.
Strike PhantomNet_608877a9	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 608877a9e11101da53bce99b0effc75b.
Strike PhantomNet_66007a1c	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 66007a1ca6d07ebb4ed85bf82e79719d.
Strike PhantomNet_7de7febe	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 7de7feb6bed06c49efb4e2c3dd23e1.
Strike PhantomNet_81159738	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 81159738f7ffb50d5bc3c75e5e0ac546.

<b>Name</b>	<b>Description</b>
Strike PhantomNet_b6e3894c	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is b6e3894c17fb05db754a61ac9a0e5925.
Strike PhantomNet_bbf9216	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is bbf92161cb71825a16e49e2aa4d2750.
Strike PhantomNet_f21b63dd	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is f21b63ddd7d2a773eb21a065015cdd01.
Strike PuTTYRider_02b3a5f0	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is 02b3a5f0121fab02f22173c9e738fee6.
Strike PuTTYRider_0e041de4	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is 0e041de4bca18fdfa54c525ae524e018.

<b>Name</b>	<b>Description</b>
Strike PuTTYRider_4e61cfa7	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is 4e61cfa7d791788ae557319e83c63fb4.
Strike PuTTYRider_7b1854a4	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is 7b1854a4bd691db129459ac6f50668b6.
Strike PuTTYRider_8eb873ad	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is 8eb873ad112121cdfd0cc72688aa229f.
Strike PuTTYRider_8ed690f6	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is 8ed690f6438133f4661465253daba3bc.
Strike PuTTYRider_93b46063	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is 93b460635a4015d04bfae9eb3cd537cc.

<b>Name</b>	<b>Description</b>
Strike PuTTYRider_bb50383e	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is bb50383eac05377d7feae5b9c3024550.
Strike PuTTYRider_e48431ba	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is e48431ba5aa7a42ae0a32eb7d859d7a4.
Strike PuTTYRider_eb119087	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is eb119087d7395ca0e9c32e5fc3bcbc3b.
Strike Qilin_0f73b467	This strike sends a malware sample known as Qilin. Qilin is a malware that is used in conjunction with other malicious software to carry out targeted attacks. It is usually delivered via spear-phishing emails or waterhole attacks, and is often seen in combination with the PlugX and Quasar RATs. Once executed, Qilin creates a backdoor into the infected system, allowing for further exploitation. Its key capabilities include launching additional payloads, achieving persistence, and performing reconnaissance on the infected system. The MD5 hash of this Qilin sample is 0f73b467ff03f9224c024f4eb3aecedb.
Strike Qilin_1c0cb55d	This strike sends a malware sample known as Qilin. Qilin is a malware that is used in conjunction with other malicious software to carry out targeted attacks. It is usually delivered via spear-phishing emails or waterhole attacks, and is often seen in combination with the PlugX and Quasar RATs. Once executed, Qilin creates a backdoor into the infected system, allowing for further exploitation. Its key capabilities include launching additional payloads, achieving persistence, and performing reconnaissance on the infected system. The MD5 hash of this Qilin sample is 1c0cb55d3a8d544ab0bd7d81d2985089.

<b>Name</b>	<b>Description</b>
Strike Qilin_227f14f4	This strike sends a malware sample known as Qilin. Qilin is a malware that is used in conjunction with other malicious software to carry out targeted attacks. It is usually delivered via spear-phishing emails or waterhole attacks, and is often seen in combination with the PlugX and Quasar RATs. Once executed, Qilin creates a backdoor into the infected system, allowing for further exploitation. Its key capabilities include launching additional payloads, achieving persistence, and performing reconnaissance on the infected system. The MD5 hash of this Qilin sample is 227f14f4c3aa35b9fb279f52c73b2e1e.
Strike Qilin_59c3334d	This strike sends a malware sample known as Qilin. Qilin is a malware that is used in conjunction with other malicious software to carry out targeted attacks. It is usually delivered via spear-phishing emails or waterhole attacks, and is often seen in combination with the PlugX and Quasar RATs. Once executed, Qilin creates a backdoor into the infected system, allowing for further exploitation. Its key capabilities include launching additional payloads, achieving persistence, and performing reconnaissance on the infected system. The MD5 hash of this Qilin sample is 59c3334d184159008cd45355b436d9a8.
Strike Qilin_bb8bdb3e	This strike sends a malware sample known as Qilin. Qilin is a malware that is used in conjunction with other malicious software to carry out targeted attacks. It is usually delivered via spear-phishing emails or waterhole attacks, and is often seen in combination with the PlugX and Quasar RATs. Once executed, Qilin creates a backdoor into the infected system, allowing for further exploitation. Its key capabilities include launching additional payloads, achieving persistence, and performing reconnaissance on the infected system. The MD5 hash of this Qilin sample is bb8bdb3e8c92e97e2f63626bc3b254c4.
Strike Qilin_e2c05908	This strike sends a malware sample known as Qilin. Qilin is a malware that is used in conjunction with other malicious software to carry out targeted attacks. It is usually delivered via spear-phishing emails or waterhole attacks, and is often seen in combination with the PlugX and Quasar RATs. Once executed, Qilin creates a backdoor into the infected system, allowing for further exploitation. Its key capabilities include launching additional payloads, achieving persistence, and performing reconnaissance on the infected system. The MD5 hash of this Qilin sample is e2c059083926ec2c219cebcfa4a49453.
Strike QuirkyLoader_10e8d5ac	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 10e8d5ac2618249893621ed0a41352cc.

<b>Name</b>	<b>Description</b>
Strike QuirkyLoader_1b636f0a	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 1b636f0ac4cc6de7d4471e657335bf37.
Strike QuirkyLoader_26d4d38a	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 26d4d38a8f1d00fe4a1d62e300b98d80.
Strike QuirkyLoader_2c4da8bd	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 2c4da8bd3cbb9c94aa333bd5c576506b.
Strike QuirkyLoader_4116b369	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 4116b3691852c2c165e38b8af52ea578.
Strike QuirkyLoader_57868447	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 57868447d89fda05231bb6d9cf9bb8f.

<b>Name</b>	<b>Description</b>
Strike QuirkyLoader_6f071d1b	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 6f071d1b91536627b9ef8ea725b810fb.
Strike QuirkyLoader_74373fbc	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 74373fbce1940202e3cc0c25efbf90bf.
Strike QuirkyLoader_796f3de2	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 796f3de2f22819c86aefd4dab652522d.
Strike QuirkyLoader_8907fef4	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 8907fef409d8684cdd0c48043933aa0b.
Strike QuirkyLoader_99f78e41	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 99f78e41cc5f086519626b8dfbb76f54.

<b>Name</b>	<b>Description</b>
Strike QuirkyLoader_b013e43b	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is b013e43be40c6c6608279f23733321b2.
Strike QuirkyLoader_b579d382	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is b579d3822cded4babedc13ae9b786d3e.
Strike QuirkyLoader_e6b379aa	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is e6b379aa359195e02462ebd5fa1f1e9b.
Strike QuirkyLoader_eac607ad	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is eac607ad42e1e1b8dd9f7f85cc511ec3.
Strike SDK_13ac2635	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 13ac2635f70981a33bc422b7b8a8b5fd.

<b>Name</b>	<b>Description</b>
Strike SDK_1afd6a2e	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 1afd6a2e005334df2b24175ec80d0742.
Strike SDK_287ddfa3	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 287ddfa34525de0556c521cf21115b9a.
Strike SDK_3c0eaeb3	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 3c0eaeb351d17d8ac1d42bdcf41178ad.
Strike SDK_6dab8bad	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 6dab8bad4349055397aa35f1a48e9c90.
Strike SDK_76d40886	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 76d40886dce0d57b99f7008af5e19bf.

<b>Name</b>	<b>Description</b>
Strike SDK_78ebd502	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 78ebd502ed1221202398623fb8ee2dd9.
Strike SDK_8823adc0	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 8823adc0960b86986aa346c119bd41f7.
Strike SDK_91827d2f	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 91827d2f3ab34de6b5857dab88c9a363.
Strike SDK_9589482a	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 9589482ad6c81182968a9fcba0f7ceed.
Strike SDK_963e8b9f	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 963e8b9f4400e7ad7f73cdd14b5f1b87.

<b>Name</b>	<b>Description</b>
Strike SDK_9967784e	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 9967784e01447928148ac24d7e4c8f3d.
Strike SDK_a4027650	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is a40276505836397427fc37e979a1f353.
Strike SDK_b253302c	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is b253302c5936ef4eb8c3fbe74026ded6.
Strike SDK_b6442835	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is b644283582d909cde0e9bf4baf42fd16.
Strike SDK_c32c66aa	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is c32c66aae96d1a48ecf0e37f2be29ef5.

<b>Name</b>	<b>Description</b>
Strike SDK_e1a20e6d	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is e1a20e6d49c837bac9d2b56aae71db40.
Strike SDK_e9754692	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is e9754692659f4d39c4e8d5fe6cb51973.
Strike SDK_f2af8db5	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is f2af8db568f135cd9a788b7caff4d517.
Strike Sidewinder_0aea0695	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 0aea06959cdd43e43f8b9d4625267398.
Strike Sidewinder_243bfa39	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 243bfa3990d9b263e6ac1265735f79be.

<b>Name</b>	<b>Description</b>
Strike Sidewinder_6fbc9a6f	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 6fbc9a6f81f99e7c32529ab9835cbc0.
Strike Sidewinder_81dfbdb2	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 81dfbdb2056db1b33440e8d3d57511d5.
Strike Sidewinder_88109f66	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 88109f669191ff1809c662a6691dcfc7.
Strike Sidewinder_888b6313	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 888b6313812112cae5c16d2e39a74d30.
Strike Sidewinder_99c545ba	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 99c545ba0a638a1ccd48e72372ea4e88.

<b>Name</b>	<b>Description</b>
Strike Sidewinder_9e10fea1	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 9e10fea142ce2fbc729f2bb30178ba79.
Strike Sidewinder_b8819140	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is b881914069d0dbbedd70cd8319541d7c.
Strike Sidewinder_d2b300dc	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is d2b300dce04690bc227cd7e7f0bb07a9.
Strike Sidewinder_e567f387	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is e567f3877e3a206d31629409ed7e1910.
Strike UAC-0057_0767b2a1	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 0767b2a1b9c596ec1865440e71b88f2d.

<b>Name</b>	<b>Description</b>
Strike UAC-0057_1520993f	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 1520993f3ad3bc307a40e7e056d364cb.
Strike UAC-0057_1541d989	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 1541d989d8908b55d7a08d3683579027.
Strike UAC-0057_38580294	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 38580294995d09e2ceacaf17fb03d609.
Strike UAC-0057_408d3148	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 408d3148fbb750a9c0b0e3c4a6017d67.
Strike UAC-0057_47c1349e	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 47c1349ec74f11b5b17de51ede1c5ec7.

<b>Name</b>	<b>Description</b>
Strike UAC-0057_5389e211	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 5389e211ec37519039d6aea8851a6254.
Strike UAC-0057_60fc5ef9	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 60fc5ef9e8de4b663cf2c38e040f4ac0.
Strike UAC-0057_65a7afe1	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 65a7afe1af0fe1ef78af70267e01fff4.
Strike UAC-0057_75af8b50	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 75af8b50c5939b4186108d0ac24a9cdc.
Strike UAC-0057_7c202bc0	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 7c202bc012974783beacf526409f30d8.

<b>Name</b>	<b>Description</b>
Strike UAC-0057_8c4f881c	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 8c4f881c12957b8e581ef7e97a61f109.
Strike UAC-0057_b63d0634	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is b63d0634d5497320ded7bea7a507b26e.
Strike UAC-0057_c5f60a8e	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is c5f60a8ea7b1ea50962f14d5291a56f1.
Strike UAC-0057_cfed77c8	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is cfed77c806dffaa7b48a17f9bc2b68bf4.
Strike UAC-0057_e21f3104	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is e21f310442347eed2210a75c1fa8e01.

<b>Name</b>	<b>Description</b>
Strike UAC-0057_e5830a1e	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is e5830a1ee8791d16939d95183a360c99.
Strike UAC-0057_eec3f959	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is eec3f9594965066db8aa5482e18618bd.
Strike UAC-0057_f7ca2539	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is f7ca25396926c6b7c35f9c86d9f79f36.
Strike UAT-8099_012dd968	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 012dd9682230ce26aefa84a9d75bedbc.
Strike UAT-8099_24762276	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 24762276a8f080a6e6d77bea05385f91.

<b>Name</b>	<b>Description</b>
Strike UAT-8099_34114faa	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 34114faa30feb8dabc8074646c8c7937.
Strike UAT-8099_37ca2f20	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 37ca2f2065f79f5b718d5e55f7dabb8e.
Strike UAT-8099_3d880c3f	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 3d880c3f1325c6d9dd7cb97c8e2180ab.
Strike UAT-8099_551c7a45	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 551c7a45ee57e666c2e1655845958db6.
Strike UAT-8099_841a5272	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 841a5272bfb67cf4c56c086e07601005.

<b>Name</b>	<b>Description</b>
Strike UAT-8099_97791d41	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 97791d414cb9e442934adae3958424e2.
Strike UAT-8099_d30b2b33	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is d30b2b33998d2498c983bfde1b99a76e.
Strike UAT-8099_db4e8d99	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is db4e8d990cb9d6ec06ad47c2311e3701.
Strike UAT-8099_ee127dbe	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is ee127dbe8daa25640c2501004f1547b0.
Strike UAT-8099_f30db5d9	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is f30db5d99477f0d2ffa2f8b578c6f1d1.

<b>Name</b>	<b>Description</b>
Strike UAT-8099_f79e154b	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is f79e154b77a248493bc4d34ea1c19547.
Strike UAT-8099_f9f87fcf	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is f9f87fcfd6ecc6d65381f97aec65f75b.
Strike UAT-8099_fef21f73	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is fef21f73ba6da0cb6221976a8fb64cdd.
Strike llm_enabled_1854a442	This strike sends a malware sample known as llm_enabled. LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this llm_enabled sample is 1854a4427eef0f74d16ad555617775ff.
Strike llm_enabled_1952345e	This strike sends a malware sample known as llm_enabled. LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this llm_enabled sample is 1952345e66e1f3173190d282f810a37d.

<b>Name</b>	<b>Description</b>
Strike llm_enabled_1a6be50d	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>1a6be50d9839d2e4dc6b028df05b334</code> .
Strike llm_enabled_2fdfdf0	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>2fdfdf0b099cc195316a85636e9636d</code> .
Strike llm_enabled_40b179e3	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>40b179e334fd12241823e4ad353bb96d</code> .
Strike llm_enabled_651d69c8	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>651d69c843f827f9ed871f595ffa15e5</code> .
Strike llm_enabled_74eb831b	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>74eb831b26a21d954261658c72145128</code> .

<b>Name</b>	<b>Description</b>
Strike llm_enabled_806f5520	This strike sends a malware sample known as llm_enabled. LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this llm_enabled sample is 806f552041f211a35e434112a0165568.
Strike llm_enabled_81cd2031	This strike sends a malware sample known as llm_enabled. LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this llm_enabled sample is 81cd20319c8f0b2ce499f9253ce0a6a8.
Strike llm_enabled_9d92b543	This strike sends a malware sample known as llm_enabled. LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this llm_enabled sample is 9d92b5436a0e75471de4b583696b33ac.
Strike llm_enabled_ac377e26	This strike sends a malware sample known as llm_enabled. LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this llm_enabled sample is ac377e26c24f50b4d9aaa933d788c18c.
Strike llm_enabled_ed229f34	This strike sends a malware sample known as llm_enabled. LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this llm_enabled sample is ed229f3442f2d45f6fdd4f3a4c552c1c.

<b>Name</b>	<b>Description</b>
Strike llm_enabled_f7cf07f2	This strike sends a malware sample known as llm_enabled. LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this llm_enabled sample is f7cf07f2bf07cfc054ac909d8ae6223d.
Strike nimbus_manticore_14d8e86 5	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is 14d8e865d3ca67b88c01f7e5d2b0862d.
Strike nimbus_manticore_3a85381 d	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is 3a85381dd880c69f40b02859cd9fd473.
Strike nimbus_manticore_7766772 5	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is 776677256087a5a0f543a6b6317cadf8.
Strike nimbus_manticore_83b7ec5f	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is 83b7ec5f0d5d6f11ba1284a3f705e98e.

<b>Name</b>	<b>Description</b>
Strike nimbus_manticore_96a9078d	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is 96a9078d97a8b2a0cdc6632b48b8a649.
Strike nimbus_manticore_b40533e6	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is b40533e67e70b7ff7bb53d34a4b9170e.
Strike nimbus_manticore_b7e4b752	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is b7e4b752adff07ac1b7b67a9be30b366.
Strike nimbus_manticore_be2bd408	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is be2bd408c615997c600871970573f023.
Strike operation_rewrite_0721efb9	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 0721efb9a3e364a372bbb4b7b7c42193.

<b>Name</b>	<b>Description</b>
Strike operation_rewrite_5ed7d3f4	<p>This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 5ed7d3f4e83c9456363c0502a7b00fac.</p>
Strike operation_rewrite_6049f6d2	<p>This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 6049f6d24d84b335ae8eb19d049e9e42.</p>
Strike operation_rewrite_6cada79f	<p>This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 6cada79fd399172f4ff55774ad1954ce.</p>
Strike operation_rewrite_728605f7	<p>This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 728605f7586642a814e900e9b2f236fb.</p>
Strike operation_rewrite_74863e3 5	<p>This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 74863e35f68f27386eb0f65528b5855a.</p>

<b>Name</b>	<b>Description</b>
Strike operation_rewrite_920a193 8	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 920a193888df5adef270d3f05e907d8b.
Strike operation_rewrite_941cf054	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 941cf0549f9246c655e77767cacb8666.
Strike operation_rewrite_97a7823 8	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 97a78238ffa97e140d05d18611979d55.
Strike operation_rewrite_a98432ed	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is a98432ed45af026f93fb450fd9ebcdda.
Strike operation_rewrite_b1760f43	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is b1760f43574b88382fcdc589ca458254.

<b>Name</b>	<b>Description</b>
Strike operation_rewrite_db3652d 4	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is db3652d42598323481d3168409b5b9bb.
Strike operation_rewrite_e50a3e80	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is e50a3e8071e49e17d4d11e98e57cddc8.
Strike operation_rewrite_e7e8240b	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is e7e8240be190f80c52fd4c8f26f61f68.
Strike operation_rewrite_eb84dc41	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is eb84dc4121511343b0336c92715cbe5.
Strike operation_rewrite_ebe4e970	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is ebe4e97053230d841d9f5fca62caf9ac.

Name	Description
Strike operation_rewrite_f4136470	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is f413647083a0701e91b5a2fc247fd586.
Strike soco404_14bf32e7	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is 14bf32e780601c6870811982648cf293.
Strike soco404_229df8da	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is 229df8dab03385371464e9a5f3ee89bd.
Strike soco404_2a26af6c	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is 2a26af6c46ffb18509397b2ec7f9389a.
Strike soco404_35b66458	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is 35b6645859a2fcd674042e284879be11.
Strike soco404_6a267dfa	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is 6a267dfa08378eab14650b8d5fd6171.
Strike soco404_71309198	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is 713091980135a30a452b34026d949890.

<b>Name</b>	<b>Description</b>
Strike soco404_7feedc2c	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is 7feedc2cd91f037d1bcd285e6f1341b.
Strike soco404_ac00592c	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is ac00592cb93fbb64c26b7f99cfcb80be.
Strike soco404_bb8fbe0f	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is bb8fbe0f257508c78df00252de2fa48c.
Strike soco404_bd8ce6bd	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is bd8ce6bd59b1f648e0ac38e575780453.
Strike soco404_c95ab34d	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is c95ab34d79740f5fa5fdc211c35eb5ea.
Strike soco404_ca125aba	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is ca125aba3e130e2d6a122fcc76461fdc.
Strike soco404_d2226fa9	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is d2226fa9e050f8fd5fe3d4aae27d3406.
Strike soco404_fa904f9d	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is fa904f9d5abecd5e62645b115f30d971.

# Full Content List

## All Exploits (3107)

Name	References	Description
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Binary Tree Encryption-Decryption - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a code-style jailbreak template, and the encryption method employed is binary tree encoding, where the original prompt is structured into a binary tree format. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Binary Tree Encryption-Decryption - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a code-style jailbreak template, and the encryption method employed is binary tree encoding, where the original prompt is structured into a binary tree format. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Binary Tree Encryption-Decryption - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a code-style jailbreak template, and the encryption method employed is binary tree encoding, where the original prompt is structured into a binary tree format. Target LLM: OpenAI
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Binary Tree Encryption Only - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a code-style jailbreak template, and the encryption method employed is binary tree encoding, where the original prompt is structured into a binary tree format. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Binary Tree Encryption Only - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a code-style jailbreak template, and the encryption method employed is binary tree encoding, where the original prompt is structured into a binary tree format. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Binary Tree Encryption Only - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a code-style jailbreak template, and the encryption method employed is binary tree encoding, where the original prompt is structured into a binary tree format. Target LLM: OpenAI

Name	References	Description
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Length Encryption-Decryption - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a code-style jailbreak template, and the encryption method employed is based on word length, where we arrange words and their lengths in key-value fashion and sort them lexicographically. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Length Encryption-Decryption - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a code-style jailbreak template, and the encryption method employed is based on word length, where we arrange words and their lengths in key-value fashion and sort them lexicographically. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Length Encryption-Decryption - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a code-style jailbreak template, and the encryption method employed is based on word length, where we arrange words and their lengths in key-value fashion and sort them lexicographically. Target LLM: OpenAI
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Length Encryption Only - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a code-style jailbreak template, and the encryption method employed is based on word length, where we arrange words and their lengths in key-value pair fashion and sort them lexicographically. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Length Encryption Only - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a code-style jailbreak template, and the encryption method employed is based on word length, where we arrange words and their lengths in key-value pair fashion and sort them lexicographically. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Length Encryption Only - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a code-style jailbreak template, and the encryption method employed is based on word length, where we arrange words and their lengths in key-value pair fashion and sort them lexicographically. Target LLM: OpenAI

Name	References	Description
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with No Encryption - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. This strike uses a code-style jailbreak template, the embedded prompt is sent in plain text without any encryption or obfuscation. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with No Encryption - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. This strike uses a code-style jailbreak template, the embedded prompt is sent in plain text without any encryption or obfuscation. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with No Encryption - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. This strike uses a code-style jailbreak template, the embedded prompt is sent in plain text without any encryption or obfuscation. Target LLM: OpenAI
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Odd-Even Encryption- Decryption - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a code-style jailbreak template, and the encryption method employed is odd-even, where words at odd and even indices are extracted and the two sets are placed one after the other. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Odd-Even Encryption- Decryption - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a code-style jailbreak template, and the encryption method employed is odd-even, where words at odd and even indices are extracted and the two sets are placed one after the other. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Odd-Even Encryption- Decryption - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a code-style jailbreak template, and the encryption method employed is odd-even, where words at odd and even indices are extracted and the two sets are placed one after the other. Target LLM: OpenAI
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Odd-Even Encryption Only - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a code-style jailbreak template, and the encryption method employed is odd-even, where words at odd and even indices are extracted and the two sets are placed one after the other. Target LLM: Gemini

Name	References	Description
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Odd-Even Encryption Only - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a code-style jailbreak template, and the encryption method employed is odd-even, where words at odd and even indices are extracted and the two sets are placed one after the other. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Odd-Even Encryption Only - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a code-style jailbreak template, and the encryption method employed is odd-even, where words at odd and even indices are extracted and the two sets are placed one after the other. Target LLM: OpenAI
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Reverse Encryption-Decryption - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a code-style jailbreak template, and the encryption method employed is reverse order, where the order of words in the original prompt is reversed. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Reverse Encryption-Decryption - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a code-style jailbreak template, and the encryption method employed is reverse order, where the order of words in the original prompt is reversed. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Reverse Encryption-Decryption - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a code-style jailbreak template, and the encryption method employed is reverse order, where the order of words in the original prompt is reversed. Target LLM: OpenAI
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Reverse Encryption Only - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a code-style jailbreak template, and the encryption method employed is reverse order, where the order of words in the original prompt is reversed. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Reverse Encryption Only - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a code-style jailbreak template, and the encryption method employed is reverse order, where the order of words in the original prompt is reversed. Target LLM: Grok

Name	References	Description
Strike AI LLM CodeChameleon Prompt Injection Using Code Template with Reverse Encryption Only - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a code-style jailbreak template, and the encryption method employed is reverse order, where the order of words in the original prompt is reversed. Target LLM: OpenAI
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Binary Tree Encryption-Decryption - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a text-style jailbreak template, and the encryption method employed is binary tree encoding, where the original prompt is structured into a binary tree format. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Binary Tree Encryption-Decryption - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a text-style jailbreak template, and the encryption method employed is binary tree encoding, where the original prompt is structured into a binary tree format. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Binary Tree Encryption-Decryption - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a text-style jailbreak template, and the encryption method employed is binary tree encoding, where the original prompt is structured into a binary tree format. Target LLM: OpenAI
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Binary Tree Encryption Only - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a text-style jailbreak template, and the encryption method employed is binary tree encoding, where the original prompt is structured into a binary tree format. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Binary Tree Encryption Only - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a text-style jailbreak template, and the encryption method employed is binary tree encoding, where the original prompt is structured into a binary tree format. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Binary Tree Encryption Only - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a text-style jailbreak template, and the encryption method employed is binary tree encoding, where the original prompt is structured into a binary tree format. Target LLM: OpenAI

Name	References	Description
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Length Encryption-Decryption - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a text-style jailbreak template, and the encryption method employed is based on word length, where we arrange words and their lengths in key-value pair fashion and sort them lexicographically. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Length Encryption-Decryption - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a text-style jailbreak template, and the encryption method employed is based on word length, where we arrange words and their lengths in key-value pair fashion and sort them lexicographically. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Length Encryption-Decryption - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a text-style jailbreak template, and the encryption method employed is based on word length, where we arrange words and their lengths in key-value pair fashion and sort them lexicographically. Target LLM: OpenAI
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Length Encryption Only - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a text-style jailbreak template, and the encryption method employed is based on word length, where we arrange words and their lengths in key-value pair fashion and sort them lexicographically. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Length Encryption Only - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a text-style jailbreak template, and the encryption method employed is based on word length, where we arrange words and their lengths in key-value pair fashion and sort them lexicographically. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Length Encryption Only - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a text-style jailbreak template, and the encryption method employed is based on word length, where we arrange words and their lengths in key-value pair fashion and sort them lexicographically. Target LLM: OpenAI

Name	References	Description
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with No Encryption - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. This strike uses a text-style jailbreak template, the embedded prompt is sent in plain text without any encryption or obfuscation. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with No Encryption - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. This strike uses a text-style jailbreak template, the embedded prompt is sent in plain text without any encryption or obfuscation. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with No Encryption - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. This strike uses a text-style jailbreak template, the embedded prompt is sent in plain text without any encryption or obfuscation. Target LLM: OpenAI
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Odd-Even Encryption- Decryption - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a text-style jailbreak template, and the encryption method employed is odd-even, where words at odd and even indices are extracted and the two sets are placed one after the other. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Odd-Even Encryption- Decryption - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a text-style jailbreak template, and the encryption method employed is odd-even, where words at odd and even indices are extracted and the two sets are placed one after the other. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Odd-Even Encryption- Decryption - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a text-style jailbreak template, and the encryption method employed is odd-even, where words at odd and even indices are extracted and the two sets are placed one after the other. Target LLM: OpenAI
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Odd-Even Encryption Only - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a text-style jailbreak template, and the encryption method employed is odd-even, where words at odd and even indices are extracted and the two sets are placed one after the other. Target LLM: Gemini

Name	References	Description
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Odd-Even Encryption Only - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a text-style jailbreak template, and the encryption method employed is odd-even, where words at odd and even indices are extracted and the two sets are placed one after the other. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Odd-Even Encryption Only - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a text-style jailbreak template, and the encryption method employed is odd-even, where words at odd and even indices are extracted and the two sets are placed one after the other. Target LLM: OpenAI
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Reverse Encryption-Decryption - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a text-style jailbreak template, and the encryption method employed is reverse order, where the order of words in the original prompt is reversed. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Reverse Encryption-Decryption - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a text-style jailbreak template, and the encryption method employed is reverse order, where the order of words in the original prompt is reversed. Target LLM: Grok
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Reverse Encryption-Decryption - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding its corresponding decryption logic within the instructions. The LLM processes this logic to reconstruct and execute the original query. This strike uses a text-style jailbreak template, and the encryption method employed is reverse order, where the order of words in the original prompt is reversed. Target LLM: OpenAI
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Reverse Encryption Only - Gemini		This strike sends a jailbreak prompt known as CodeChameleon to the Gemini LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a text-style jailbreak template, and the encryption method employed is reverse order, where the order of words in the original prompt is reversed. Target LLM: Gemini
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Reverse Encryption Only - Grok		This strike sends a jailbreak prompt known as CodeChameleon to the Grok LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a text-style jailbreak template, and the encryption method employed is reverse order, where the order of words in the original prompt is reversed. Target LLM: Grok

Name	References	Description
Strike AI LLM CodeChameleon Prompt Injection Using Text Template with Reverse Encryption Only - OpenAI		This strike sends a jailbreak prompt known as CodeChameleon to the OpenAI LLM. The technique involves encrypting the original prompt and embedding it within the instructions. This strike uses a text-style jailbreak template, and the encryption method employed is reverse order, where the order of words in the original prompt is reversed. Target LLM: OpenAI
Strike Apache Struts REST Plugin OGNL Expression Code Execution Vulnerability	CVE: 2016-3087	This strike exploits a code execution vulnerability in Apache Struts. The vulnerability resides in the handleDynamicMethodInvocation() method of the RestActionMapper class when processing OGNL expressions with Direct Method Invocation enabled. A remote attacker can leverage this flaw by sending a crafted HTTP request, allowing arbitrary code execution with the privileges of the server.
Strike Moxa SoftCMS getcaminfo.asp VVID Parameter SQL Injection Vulnerability	CVE: 2016-5792	This strike exploits a SQL injection vulnerability in Moxa SoftCMS. The vulnerability exists due to improper sanitization of user-supplied input in the VVID parameter of the getcaminfo.asp page. A remote attacker could leverage this flaw by sending a specially crafted HTTP request, potentially leading to unauthorized database access, information disclosure, and remote code execution.
Strike Oracle Identity Manager Default Credentials Vulnerability	CVE: 2017-10151	This strike exploits an authentication weakness vulnerability in Oracle Identity Manager. The vulnerability exists due to the presence of default credentials in the WebLogic Server Administration Console and Enterprise Manager interfaces. A remote attacker can leverage this flaw to gain administrator-level privileges on the target system.
Strike HPE Intelligent Management Center FileDownloadServlet Directory Traversal Vulnerability	CVE: 2017-5795	This strike exploits a directory traversal vulnerability in HPE Intelligent Management Center. The vulnerability resides in the FileDownloadServlet due to improper sanitization of the fileName parameter in HTTP GET requests. A remote attacker can leverage this flaw to access and disclose arbitrary file contents from the server.
Strike Advantech WebAccess WADashboard Arbitrary File Overwrite Vulnerability	CVE: 2018-15705	This strike exploits an arbitrary file overwrite vulnerability in Advantech WebAccess SCADA WADashboard. The vulnerability exists due to improper validation of the folderpath parameter in HTTP requests, allowing directory traversal sequences to bypass restrictions. A remote, authenticated attacker can leverage this flaw to write arbitrary files to the server's file system, potentially leading to remote code execution.
Strike Zoho ManageEngine OpManager SQL Injection in Alarms API	CVE: 2018-20338	This strike exploits a SQL injection vulnerability in Zoho ManageEngine OpManager. The vulnerability resides in the insufficient validation of the "filters" parameter in HTTP requests to the listAlarms API. A remote, authenticated attacker could leverage this flaw by sending crafted HTTP requests containing malicious SQL queries, leading to arbitrary SQL code execution on the application's database.
Strike Schneider Electric IIoT Monitor Server downloadCSV.jsp Directory Traversal Vulnerability	CVE: 2018-7835	This strike exploits a directory traversal vulnerability in Schneider Electric IIoT Monitor Server. The vulnerability exists due to improper validation of the file parameter in requests to the downloadCSV.jsp endpoint. A remote, unauthenticated attacker could leverage this flaw to access and disclose the contents of arbitrary files accessible by the SYSTEM user.

Name	References	Description
Strike Zoho ManageEngine Applications Manager SQL Injection in Popup_SLA.jsp (sid Parameter)	CVE: 2019-11448	This strike exploits a SQL injection vulnerability in Zoho ManageEngine Applications Manager. The vulnerability resides in the improper validation of the "sid" parameter in the Popup_SLA.jsp Java class. A remote, unauthenticated attacker could leverage this flaw to execute arbitrary SQL commands, potentially leading to database manipulation and remote code execution in the context of the application.
Strike HPE Intelligent Management Center Expression Language Injection Vulnerability cve_2019_11943	CVE: 2019-11943	This strike exploits an Expression Language injection vulnerability in HPE Intelligent Management Center. The vulnerability resides in the improper validation of the beanName parameter within the SoapConfigBean class. Exploiting this flaw allows a remote, authenticated attacker to execute arbitrary code on the target system with SYSTEM-level privileges.
Strike Squid Proxy Digest Authentication Nonce Pointer Disclosure Vulnerability	CVE: 2019-18679	This strike exploits an information disclosure vulnerability in Squid Proxy. The vulnerability resides in the improper construction of the nonce value used in HTTP Digest authentication. A remote attacker could exploit this vulnerability to obtain leaked pointer addresses, potentially bypassing ASLR and facilitating further attacks.
Strike CoDeSys V3 CmpWebServer Heap Buffer Overflow Vulnerability	CVE: 2019-18858	This strike exploits a heap-based buffer overflow vulnerability in the CoDeSys V3 runtime system's web server. The vulnerability arises from improper validation of user-supplied data in the HTTP header "3S-Repl-Content" when processing requests to the /WebVisuV3 endpoint. A remote, unauthenticated attacker can exploit this flaw by sending specially crafted HTTP requests, potentially leading to arbitrary code execution in the context of the server process.
Strike rConfig devices.inc.php SQL Injection Vulnerability	CVE: 2019-19207	This strike exploits an SQL injection vulnerability in the rConfig Network Device Configuration Tool. The vulnerability exists due to improper sanitization of the searchColumn and searchField parameters in the devices.inc.php script. A remote, authenticated attacker can leverage this flaw by sending specially crafted HTTP requests, potentially leading to the execution of arbitrary SQL commands on the database of the target server.
Strike HPE Intelligent Management Center Expression Language Injection Vulnerability	CVE: 2019-5370	This strike exploits an Expression Language injection vulnerability in HPE Intelligent Management Center. The vulnerability resides in the IctTableExportToCSVBean class, specifically in the handling of the beanName HTTP request parameter. A remote attacker, after bypassing authentication or using valid credentials, can exploit this flaw by sending a crafted request, leading to arbitrary code execution with SYSTEM-level privileges.
Strike rConfig compliancepolicies.inc.php Unauthenticated SQL Injection Vulnerability	CVE: 2020-10546	This strike exploits a SQL injection vulnerability in the rConfig Network Device Configuration Tool. The vulnerability exists due to insufficient input validation in the compliancepolicies.inc.php script when processing HTTP request parameters. A remote, unauthenticated attacker can leverage this flaw to execute arbitrary SQL commands on the database, potentially leading to unauthorized data manipulation or access.

Name	References	Description
Strike OpenEMR phpGACL edit_group.php SQL Injection Vulnerability	CVE: 2020-13568	This strike exploits a SQL injection vulnerability in the OpenEMR phpGACL edit_group.php script. The vulnerability arises from improper validation of user-supplied input in the "parent_id" parameter during HTTP POST requests. A remote authenticated attacker can leverage this flaw to execute arbitrary SQL commands, potentially leading to the disclosure of sensitive information and further system compromise.
Strike Zoho ManageEngine OpManager Directory Traversal Vulnerability cve_2020_13818	CVE: 2020-13818	This strike exploits a directory traversal vulnerability in Zoho ManageEngine OpManager. The vulnerability resides in the improper validation of URI paths within the OpmSkipFilter::doFilter() method. A remote, unauthenticated attacker could leverage this flaw by sending specially crafted requests, potentially leading to arbitrary file read and disclosure of sensitive information on the target server.
Strike Cacti color.php SQL Injection Vulnerability	CVE: 2020-14295	This strike exploits a SQL injection vulnerability in Cacti. The vulnerability exists due to improper sanitization of the "filter" parameter in the color.php script. A remote, authenticated attacker could leverage this flaw to execute arbitrary SQL commands on the database, potentially leading to remote code execution on the target server.
Strike Zoho ManageEngine Applications Manager SQL Injection in AlertRes_Mtrgrp.jsp	CVE: 2020-15533	This strike exploits a SQL injection vulnerability in Zoho ManageEngine Applications Manager. The vulnerability exists due to insufficient validation of the "sid" parameter in the AlertRes_Mtrgrp.jsp servlet. A remote, unauthenticated attacker could leverage this flaw to execute arbitrary SQL commands, potentially leading to database manipulation and arbitrary code execution with SYSTEM privileges.
Strike Oracle Business Intelligence AMF Insecure Deserialization Vulnerability	CVE: 2020-2950	This strike exploits an insecure deserialization vulnerability in Oracle Business Intelligence. The vulnerability is located in the handling of AMF3 objects marked as externalizable within the BiRemotingServlet component. Exploiting this vulnerability allows a remote, unauthenticated attacker to execute arbitrary code in the security context of the affected server.
Strike Zoho ManageEngine Applications Manager SQL Injection Vulnerability in UriCollector Class	CVE: 2020-35765	This strike exploits a SQL injection vulnerability in Zoho ManageEngine Applications Manager. The vulnerability resides in the improper validation of the `resourceid` parameter within the `doFilter()` method of the `UriCollector` Java class. A remote, authenticated attacker could leverage this flaw by sending a crafted HTTP request, leading to the execution of arbitrary SQL statements and potentially arbitrary code in the context of the SYSTEM user.
Strike Rockwell Automation FactoryTalk RNADiagnosticsSrv Insecure Deserialization	CVE: 2020-6967	This strike exploits an insecure deserialization vulnerability in Rockwell Automation FactoryTalk Diagnostics. The vulnerability resides in the RNADiagnosticsSrv.exe component, specifically in the OnStart() method, which improperly handles serialized data. A remote, unauthenticated attacker could exploit this vulnerability by sending a maliciously crafted serialized object, leading to arbitrary code execution under the SYSTEM security context.

Name	References	Description
Strike Jenkins Generic Webhook Trigger Plugin XXE Vulnerability	CVE: 2021-21669	This strike exploits an XML External Entity (XXE) vulnerability in the Jenkins Generic Webhook Trigger Plugin. The vulnerability resides in the resolveXPath function, which improperly handles XML data in HTTP POST requests. A remote authenticated attacker with specific permissions could exploit this flaw to access and disclose the contents of arbitrary files readable by the Jenkins server.
Strike Advantech R-SeeNet ping.php Command Injection Vulnerability	CVE: 2021-21805	This strike exploits a command injection vulnerability in Advantech R-SeeNet. The vulnerability exists due to insufficient validation of the "hostname" parameter in the ping.php script. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted HTTP request, leading to arbitrary command execution with the privileges of the web server on the target system.
Strike Oracle E-Business Suite Sales Offline Infinite Loop Denial of Service Vulnerability	CVE: 2021-2190	This strike exploits an infinite loop vulnerability in the Sales Offline component of Oracle E-Business Suite. The vulnerability is located in the improper handling of HTTP POST requests with a Content-Length header value of 0 in the aslAuthincps.jsp file. Exploiting this vulnerability allows a remote, unauthenticated attacker to cause excessive CPU usage, potentially leading to denial of service conditions on the target server.
Strike Oracle E-Business Suite Knowledge Management Stored Cross-Site Scripting Vulnerability	CVE: 2021-2198	This strike exploits a stored cross-site scripting vulnerability in Oracle E-Business Suite Knowledge Management. The vulnerability resides in the improper sanitization of user-supplied input when handling time period definitions in JSP files. An authenticated attacker with administrative privileges could exploit this flaw to execute arbitrary script code in the browsers of users visiting the affected page.
Strike Advantech iView SQL Injection Vulnerability in ZTPConfigTable	CVE: 2021-22654	This strike exploits a SQL injection vulnerability in Advantech iView. The vulnerability exists due to insufficient validation of user-supplied input in the ZTPConfigTable Java class when processing HTTP request parameters. A remote, unauthenticated attacker could leverage this flaw by sending specially crafted requests, potentially leading to the execution of arbitrary SQL commands, unauthorized data access, or further system compromise.
Strike Eaton IPM Arbitrary File Deletion via Directory Traversal	CVE: 2021-23278	This strike exploits an arbitrary file deletion vulnerability in Eaton Intelligent Power Manager. The vulnerability exists due to insufficient input validation in the handling of HTTP parameters in the maps_srv.js and node_upgrade_srv.js scripts. A remote, authenticated attacker could leverage this flaw to delete arbitrary files on the target system, potentially leading to system compromise.
Strike Eaton Intelligent Power Management Arbitrary File Deletion via Directory Traversal	CVE: 2021-23279	This strike exploits an arbitrary file deletion vulnerability in Eaton Intelligent Power Management. The vulnerability resides in the meta_driver_srv.js script due to insufficient input validation of HTTP request parameters. A remote, unauthenticated attacker can exploit this flaw to delete arbitrary files on the target system, potentially leading to system compromise.

Name	References	Description
Strike Oracle BI Publisher JNDI Injection Vulnerability in SchedulerConfigPage11g	CVE: 2021-2391	This strike exploits a JNDI injection vulnerability in Oracle Business Intelligence Publisher. The vulnerability exists due to insufficient validation of the DB.CFG.JNDIName HTTP request parameter in the SchedulerConfigPage11g class. A remote, authenticated attacker can leverage this flaw by sending a specially crafted request, leading to the execution of arbitrary code on the server through the retrieval of a malicious serialized object.
Strike Oracle Business Intelligence Arbitrary File Upload Vulnerability	CVE: 2021-2392	This strike exploits an arbitrary file upload vulnerability in Oracle Business Intelligence. The vulnerability exists due to insufficient validation of the filename parameter in the UploadFndDBCPage class. A remote, authenticated attacker could leverage this flaw to upload malicious files, potentially leading to privilege escalation or denial of service.
Strike Oracle BI Publisher JNDI Injection Vulnerability in UpdateConnectionServlet	CVE: 2021-2396	This strike targets a JNDI injection vulnerability in Oracle Business Intelligence Publisher. The issue arises from improper sanitization of the JNDINameField parameter in HTTP requests to the UpdateConnectionServlet. A remote, authenticated attacker could exploit this flaw to trigger a JNDI lookup on an attacker-controlled server, potentially leading to the execution of arbitrary code on the affected system.
Strike Apache OFBiz Insecure Deserialization Vulnerability	CVE: 2021-26295	This strike exploits an insecure deserialization vulnerability in Apache OFBiz. The vulnerability arises from improper handling of serialized objects within SOAP requests. A remote, unauthenticated attacker can exploit this flaw by sending a crafted payload, leading to arbitrary code execution on the affected system.
Strike Zoho ManageEngine AD SelfService Plus Command Injection Vulnerability	CVE: 2021-28958	This strike exploits a command injection vulnerability in Zoho ManageEngine AD SelfService Plus. The vulnerability arises from improper sanitization of user-supplied input during password change requests. A remote attacker could leverage this flaw to execute arbitrary commands on the server with the privileges of the web application.
Strike Apache OFBiz Insecure Deserialization Vulnerability cve_2021_30128	CVE: 2021-30128	This strike exploits an insecure deserialization vulnerability in Apache OFBiz. The vulnerability arises from improper validation of serialized objects within the <cus-obj> XML element in SOAP requests. A remote, unauthenticated attacker could leverage this flaw by sending a crafted payload, leading to arbitrary code execution on the affected system.
Strike Apache Tapestry ContextAssetRequestHandler Information Disclosure Vulnerability	CVE: 2021-30638	This strike exploits an information disclosure vulnerability in Apache Tapestry. The vulnerability resides in the ContextAssetRequestHandler class due to insufficient validation of user input when processing asset requests. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted HTTP request, potentially leading to unauthorized access and retrieval of sensitive files within the WEB-INF directory.

Name	References	Description
Strike Microsoft Visual Studio Code Remote-Containers Extension Remote Code Execution Vulnerability	CVE: 2021-31213	This strike exploits a remote code execution vulnerability in the Remote - Containers Extension for Microsoft Visual Studio Code. The vulnerability resides in the design flaw of the "Clone Repository in Container Volume" feature, which fails to adequately warn users about the risks of cloning untrusted repositories. A remote attacker could exploit this vulnerability by tricking a user into cloning a malicious repository, leading to the execution of arbitrary code with root-level privileges.
Strike SolarWinds Network Performance Monitor Insecure Deserialization Vulnerability	CVE: 2021-31474	This strike exploits an insecure deserialization vulnerability in SolarWinds Network Performance Monitor. The vulnerability resides in the FromJson() method of the SolarWinds.Serialization.Json.SerializationHelper class within the OrionWeb.dll component. A remote, authenticated attacker can leverage this flaw by sending a crafted serialized object to the vulnerable endpoint, leading to arbitrary code execution under the NETWORK SERVICE user context.
Strike Flarum Core Reflected and Stored Cross-Site Scripting Vulnerability	CVE: 2021-32671	This strike exploits a cross-site scripting vulnerability in the Flarum Core application. The vulnerability resides in the translation library, specifically in the preprocessParameters() method of Translators, which fails to properly sanitize HTML markup. Exploiting this vulnerability allows a remote attacker to execute arbitrary script code in the security context of the browser of any user interacting with the affected pages.
Strike Advantech iView runProViewUpgrade Command Injection Vulnerability	CVE: 2021-32930	This strike exploits a command injection vulnerability in Advantech iView. The vulnerability exists due to insufficient input validation in the `fwfilename` parameter of the `runProViewUpgrade` method within the `NetworkServlet` class. A remote, unauthenticated attacker could leverage this flaw by sending a specially crafted HTTP request, leading to the execution of arbitrary commands with SYSTEM-level privileges.
Strike SolarWinds Orion Platform RenderControl.aspx Insecure Deserialization Vulnerability	CVE: 2021-35215	This strike exploits an insecure deserialization vulnerability in the SolarWinds Orion Platform. The vulnerability resides in the RenderControl.aspx endpoint, where user-supplied JSON data is insufficiently validated. A remote, authenticated attacker can leverage this flaw to execute arbitrary code on the target system with NETWORK SERVICE privileges.
Strike SolarWinds Orion Patch Manager Insecure Deserialization Vulnerability	CVE: 2021-35216	This strike exploits an insecure deserialization vulnerability in the SolarWinds Orion Patch Manager Web Console. The vulnerability resides in the handling of the ThwackData parameter within the EditTopXX.aspx endpoint. A remote, authenticated attacker could leverage this flaw by sending a crafted serialized object, leading to remote code execution under the NETWORK SERVICE security context.
Strike OpenSSL SM2 Decryption Buffer Overflow Vulnerability	CVE: 2021-3711	This strike exploits a buffer overflow vulnerability in the OpenSSL library. The vulnerability arises from an incorrect calculation of the plaintext size during SM2 decryption in the sm2_plaintext_size function. A remote attacker can exploit this flaw by sending specially crafted SM2 encrypted data, potentially leading to denial of service conditions.

Name	References	Description
Strike Centreon csv_HostGroupLogs.php SQL Injection Vulnerability	CVE: 2021-37556	This strike exploits an SQL injection vulnerability in the Centreon Web Application. The vulnerability exists due to insufficient input validation of the "start" and "end" parameters in the csv_HostGroupLogs.php script. A remote, authenticated attacker could leverage this flaw to execute arbitrary SQL commands on the database, potentially leading to unauthorized data manipulation or further exploitation.
Strike Centreon generateImage.php SQL Injection Vulnerability	CVE: 2021-37557	This strike exploits an SQL injection vulnerability in the Centreon web application. The vulnerability is located in the generateImage.php script, specifically in the handling of the index parameter within HTTP requests. Exploiting this vulnerability allows a remote, authenticated attacker to execute arbitrary SQL commands on the database, potentially leading to unauthorized data manipulation or further compromise of the system.
Strike Zoho ManageEngine ADManager Plus Unrestricted File Upload Vulnerability	CVE: 2021-37918	This strike exploits an unrestricted file upload vulnerability in Zoho ManageEngine ADManager Plus. The vulnerability resides in the ModifyPhotoAction class, specifically in the cachePhotosBeforeImport() method, which fails to properly validate the file type of uploaded files. A remote authenticated attacker can leverage this flaw by uploading a malicious file, potentially leading to arbitrary code execution with SYSTEM-level privileges.
Strike Delta Industrial Automation DIAEnergie SQL Injection Vulnerability in HandlerAlarmGroup.aspx	CVE: 2021-38393	This strike exploits an SQL injection vulnerability in Delta Industrial Automation DIAEnergie. The vulnerability is located in the HandlerAlarmGroup.ashx endpoint due to insufficient input validation of the agid parameter. A remote, unauthenticated attacker could leverage this flaw to execute arbitrary SQL commands, potentially leading to code execution with NT SERVICE\MSSQLSERVER privileges.
Strike Zoho ManageEngine OpManager SQL Injection in getDataCollectionFailureReason Method	CVE: 2021-40493	This strike exploits a SQL injection vulnerability in Zoho ManageEngine OpManager. The vulnerability resides in the getDataCollectionFailureReason method, which fails to properly validate HTTP request parameters such as pollingObject and deviceName. A remote, authenticated attacker could leverage this flaw by sending crafted HTTP requests, leading to the execution of arbitrary SQL commands on the application's database.
Strike Zoho ManageEngine Network Configuration Manager SQL Injection Vulnerability	CVE: 2021-41081	This strike exploits a SQL injection vulnerability in Zoho ManageEngine Network Configuration Manager. The vulnerability is located in the CONFIG_SEARCH_CRITERIA parameter of the configuration search operation, where input is improperly validated. Exploiting this vulnerability allows a remote, authenticated attacker to execute arbitrary SQL commands, potentially compromising the underlying database.
Strike Delta Industrial Automation DIAEnergie Stored Cross-Site Scripting Vulnerability cve_2021_44544	CVE: 2021-44544	This strike exploits a stored cross-site scripting vulnerability in Delta Industrial Automation DIAEnergie. The vulnerability exists due to insufficient input validation in the HandlerEnergyType.ashx endpoint when processing the "name," "kid," and "descr" parameters. A remote attacker can exploit this flaw to execute arbitrary JavaScript code in the context of the victim's browser, potentially leading to unauthorized actions or data exposure.

Name	References	Description
Strike Tiny File Manager Directory Traversal and Arbitrary File Write Vulnerability	CVE: 2021-45010	This strike exploits a directory traversal vulnerability in Tiny File Manager. The vulnerability arises from insufficient validation of the "fullpath" parameter during file upload operations. A remote, authenticated attacker can leverage this flaw to perform directory traversal and arbitrary file write, potentially leading to remote code execution under the web server's security context.
Strike Apache Kylin dumpProjectDiagnosisInfo Command Injection Vulnerability	CVE: 2021-45456	This strike exploits a command injection vulnerability in Apache Kylin. The vulnerability resides in the dumpProjectDiagnosisInfo method due to improper validation of user-supplied project names. A remote authenticated attacker could leverage this flaw by crafting a malicious project name and sending it to the vulnerable REST API endpoint, leading to arbitrary command execution in the context of the server process.
Strike WordPress TI WooCommerce Wishlist Plugin item_id Blind SQL Injection Vulnerability	CVE: 2022-0412	This strike exploits a blind SQL injection vulnerability in the TI WooCommerce Wishlist Plugin for WordPress. The vulnerability exists due to improper sanitization of the user-supplied `item_id` parameter in the `get_wishlist_by_product_id()` function. Exploiting this vulnerability allows a remote, unauthenticated attacker to retrieve arbitrary information from the target database.
Strike Dolibarr ERP-CRM Menu Editor Code Injection Vulnerability	CVE: 2022-0819	This strike exploits a code injection vulnerability in the Dolibarr ERP/CRM software. The vulnerability exists due to insufficient input validation in the "Menu editor" module, specifically in the handling of the "perms" and "enabled" parameters. Exploiting this vulnerability allows a remote, authenticated attacker to execute arbitrary PHP code, potentially leading to remote code execution on the target server.
Strike WordPress Photo Gallery Plugin SQL Injection via filter_tag Parameter	CVE: 2022-1281	This strike targets a SQL injection vulnerability in the Photo Gallery plugin for WordPress. The issue arises from improper sanitization of the "filter_tag" parameter in HTTP requests. Exploiting this flaw allows a remote, unauthenticated attacker to execute arbitrary SQL commands, potentially leading to unauthorized access to sensitive database information.
Strike Pimcore GridHelperService SQL Injection Vulnerability	CVE: 2022-1429	This strike exploits a SQL injection vulnerability in Pimcore. The vulnerability exists due to improper input validation in the /grid-proxy, /get-export-jobs, and /get-batch-jobs APIs. A remote, authenticated attacker could leverage this flaw by sending specially crafted requests, potentially leading to unauthorized database access and manipulation.
Strike WordPress Events Made Easy Plugin lang Parameter SQL Injection Vulnerability	CVE: 2022-1905	This strike exploits a SQL injection vulnerability in the Events Made Easy plugin for WordPress. The vulnerability exists due to insufficient sanitization of the "lang" parameter in HTTP requests. A remote, unauthenticated attacker could leverage this flaw to execute arbitrary SQL commands, potentially leading to unauthorized access to sensitive data in the database.

Name	References	Description
Strike Lansweeper AssetActions SQL Injection Vulnerability	CVE: 2022-21210	This strike exploits an SQL injection vulnerability in Lansweeper. The vulnerability exists due to improper sanitization of user-supplied input in the "Mass Edit Assets" functionality. A remote, authenticated attacker can leverage this flaw to execute arbitrary SQL commands, potentially gaining unauthorized access to or manipulating the underlying database.
Strike Lansweeper GetAssetsByGroupId SQL Injection Vulnerability	CVE: 2022-21234	This strike exploits an SQL injection vulnerability in Lansweeper. The vulnerability exists due to improper sanitization of user-supplied input in the "order" parameter of the GetAssetsByGroupId function. A remote, authenticated attacker could leverage this flaw by sending a crafted HTTP request, potentially leading to remote code execution under the security context of the database service.
Strike Advantech iView SQL Injection in findTaskMgrItems Parameters	CVE: 2022-2135	This strike targets a SQL injection vulnerability in Advantech iView. The issue arises from insufficient input validation for the "sort_field" and "sort_type" parameters in the "findTaskMgrItems" process. Exploiting this flaw allows a remote, unauthenticated attacker to execute arbitrary SQL commands on the affected server.
Strike Advantech iView SQL Injection in set_useraccount UserName Parameter	CVE: 2022-2136	This strike targets a SQL injection vulnerability in Advantech iView. The issue arises from insufficient input validation of the UserName parameter in the set_useraccount process. Exploiting this flaw allows a remote, authenticated attacker to execute arbitrary SQL commands, potentially leading to remote code execution with SYSTEM-level privileges.
Strike Lansweeper HelpdeskSetupActions SQL Injection Vulnerability	CVE: 2022-22149	This strike exploits an SQL injection vulnerability in Lansweeper. The vulnerability exists due to improper sanitization of user-supplied input in the EditSetting() method of the HelpdeskSetupActions component. A remote, authenticated attacker can leverage this flaw to execute arbitrary SQL commands, potentially leading to remote code execution under the database service.
Strike H2 Database Console Remote Code Execution via Malformed JDBC URL	CVE: 2022-23221	This strike exploits a remote code execution vulnerability in the H2 Database Console. The vulnerability arises from improper input validation when processing specific JDBC URLs. A remote, unauthenticated attacker can exploit this flaw by sending a crafted request, potentially leading to arbitrary code execution with the privileges of the H2 process.
Strike Parse Server DatabaseController Prototype Pollution Vulnerability	CVE: 2022-24760	This strike exploits a prototype pollution vulnerability in Parse Server. The vulnerability exists due to improper input validation in the DatabaseController when handling JSON data in HTTP POST and PUT requests. A remote, unauthenticated attacker could exploit this vulnerability to inject or modify properties in Object.prototype, potentially leading to denial of service or remote code execution.
Strike WordPress WP Statistics Plugin Stored Cross-Site Scripting Vulnerability	CVE: 2022-25305	This strike exploits a stored cross-site scripting vulnerability in the WordPress WP Statistics plugin. The vulnerability exists due to insufficient input validation of the "ip," "browser," and "platform" parameters in the class-wp-statistics-visitor.php file. Exploiting this vulnerability allows a remote, unauthenticated attacker to execute arbitrary JavaScript code in the context of a user's browser.

Name	References	Description
Strike Studio-42 elFinder Directory Traversal Vulnerability	CVE: 2022-26960	This strike exploits a directory traversal vulnerability in Studio-42 elFinder. The vulnerability exists due to insufficient validation of user-supplied paths in the target and targets parameters. A remote, unauthenticated attacker can leverage this flaw to access files outside the intended web root, potentially leading to arbitrary code execution under the web server's security context.
Strike WWBN AVideo Command Injection via downloadURL Parameter	CVE: 2022-32572	This strike exploits a command injection vulnerability in WWBN AVideo. The vulnerability exists due to insufficient sanitization of the `downloadURL` parameter in HTTP requests. A remote, authenticated attacker could leverage this flaw to execute arbitrary commands on the server, potentially leading to remote code execution.
Strike Advantech iView ConfigurationServlet SQL Injection Vulnerability	CVE: 2022-3323	This strike exploits a SQL injection vulnerability in Advantech iView. The vulnerability is located in the ConfigurationServlet, specifically in the improper validation of the column_value parameter. Exploiting this vulnerability allows a remote, unauthenticated attacker to execute crafted SQL queries, potentially leading to information disclosure.
Strike Trend Micro Mobile Security web_service.dll Path Traversal Vulnerability	CVE: 2023-32521	This strike exploits a path traversal vulnerability in Trend Micro Mobile Security. The vulnerability exists due to improper validation of user-supplied file paths in the web_service.dll component. A remote, unauthenticated attacker could leverage this flaw to delete arbitrary files on the system under the security context of the IIS Anonymous Authentication account.
Strike Splunk Enterprise Arbitrary File Write via XSLT Stylesheets	CVE: 2023-46214	This strike targets an arbitrary file write vulnerability in Splunk Enterprise. The issue resides in the insufficient validation of XSLT stylesheets within the getJobAsset method of the search.py script. Exploiting this vulnerability allows a remote, authenticated attacker to create or overwrite arbitrary files, potentially leading to arbitrary code execution under the context of the Splunk process.
Strike WordPress Royal Elementor Addons Plugin Unrestricted File Upload Vulnerability	CVE: 2023-5360	This strike exploits an unrestricted file upload vulnerability in the WordPress Royal Elementor Addons and Templates plugin. The vulnerability arises from insufficient validation of user-supplied input during file upload processing. A remote attacker can leverage this flaw to upload malicious files, potentially leading to remote code execution within the context of the PHP interpreter.
Strike WordPress Ultimate Member Plugin SQL Injection via Sorting Parameter	CVE: 2024-1071	This strike exploits a time-based blind SQL injection vulnerability in the WordPress Ultimate Member plugin. The vulnerability exists due to improper input validation of the "sorting" parameter in the ajax_get_members() function. A remote, unauthenticated attacker can leverage this flaw to execute arbitrary SQL commands, potentially leading to unauthorized access to sensitive database information.
Strike ConnectWise ScreenConnect InstallExtension Directory Traversal Vulnerability	CVE: 2024-1708	This strike exploits a directory traversal vulnerability in ConnectWise ScreenConnect. The vulnerability exists due to improper validation of file paths within ZIP archives during the extension installation process. A remote attacker could leverage this flaw to execute arbitrary code on the target server by crafting malicious ZIP files.

Name	References	Description
Strike Centreon Web Virtual Metrics SQL Injection Vulnerability	CVE: 2024-55573	This strike exploits an SQL injection vulnerability in Centreon Web. The vulnerability resides in the manageVMetric method of the centreonGraph.class.php script, specifically in the handling of the rpn_function parameter. A remote, authenticated attacker could leverage this flaw by sending specially crafted requests, leading to arbitrary SQL command execution on the target database.
Strike Centreon Web updateServiceHost SQL Injection Vulnerability	CVE: 2024-5723	This strike exploits an SQL injection vulnerability in Centreon Web. The vulnerability exists due to insufficient input validation in the updateServiceHost function within the DB-Func.php script. A remote, authenticated attacker could leverage this flaw by sending specially crafted requests, leading to the execution of arbitrary SQL commands on the target database.
Strike 427BB Cookie-based Authentication Bypass (login.php)	CVE: 2006-0153 BID: 16178	This strike exploits a cross site scripting flaw in the 427BB web application.
Strike 427BB Cookie-based Authentication Bypass (getvars.php)	CVE: 2006-0153 BID: 16178	This strike exploits a cross site scripting flaw in the 427BB web application.
Strike 427BB showthread.php ForumID Parameter SQL Injection	CVE: 2006-0154 BID: 16169	This strike exploits a SQL injection flaw in the 427B web application.
Strike Microsoft Outlook Security Feature Bypass Vulnerability	CWE: 119 CVE: 2017-11774	This strike exploits a code execution vulnerability in Microsoft Outlook 2010. The vulnerability is due to improper handling of objects in memory or Microsoft Outlook security feature bypass vulnerability. By setting a crafted HTML page as Home Page in Outlook 2010, allows the attacker to execute code in the context of current user. Note: This strike simulates the opening of a malicious page at address defined in Outlook (Home Page).
Strike McAfee Web Reporter JBoss EJBInvokerServlet Marshalled Object Code Execution	CWE: 94 CVE: 2013-4810	This strike exploits in the underlining JBoss component of the McAfee Web Reporter Software. The underlining JBoss application servers is used in many enterprise webapps implementations. A flaw in authorization on the UpdateCertificateServlet class could allow a remote unauthenticated attacker to trigger arbitrary code execution with elevated privileges.
Strike Reprise License Manager HTTP licfile Buffer Overflow		This strike exploits a buffer overflow vulnerability in Reprise License Manager. The vulnerability is due to improper validation of HTTP request licfile parameter. By exploiting this vulnerability an attacker could execute arbitrary scripts on the target machine.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike WANem v2.3 Unauthorized Remote Root Access	BID: 55485	This strike exploits the Wide Area Network Emulator WANem. By combining a privilege escalation vulnerability with the dosu binary file as setuid root that executes commands supplied as its argument with the ability to inject commands into the pc parameter remotely, a user is able to gain root access remotely.
Strike ACal Cookie Based Authentication Bypass	CVE: 2006-0182	This strike exploits a cookie authentication flaw in the ACal web application.
Strike Domino Web Server Database Access - agentrunner.nsf		This strike attempts to access the /agentrunner.nsf database on a misconfigured Lotus Domino web server.
Strike Apache File Access .htgroup		This strike attempts to access an Apache configuration file over HTTP.
Strike Apache File Access .htpasswd		This strike attempts to access an Apache configuration file over HTTP.
Strike Apache File Access httpd.conf		This strike attempts to access an Apache configuration file over HTTP.
Strike Oracle 9i HTTP Server Globals.JSA Access	BID: 4034 CVE: 2002-0562	This strike attempts to access the globals.jsa file that Oracle 9i exposes in the web root.
Strike Oracle 9i HTTP Server mod_plsql Directory Traversal	BID: 3727 CVE: 2001-1217	This strike attempts to exploit a directory traversal flaw in the Oracle 9i mod_plsql module
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 1	BID: 4294 CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 2	BID: 4294 CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 3	BID: 4294 CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 4	BID: 4294  CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 5	BID: 4294  CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 6	BID: 4294  CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 7	BID: 4294  CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 8	BID: 4294  CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 9	BID: 4294  CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 10	BID: 4294  CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 11	BID: 4294  CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.
Strike Oracle 9i HTTP Server OWA_UTIL Access Variant 12	BID: 4294  CVE: 2002-0560	This strike attempts to access the OWA_UTIL PL/SQL program through the web interface of the Oracle server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle 9i HTTP Server soapConfig.xml Access	BID: 4290  CVE: 2002-0568	This strike attempts to access the Oracle 9i SOAP configuration file.
Strike Oracle 9i HTTP Server Soap Router Access	BID: 4289  CWE: 264  CVE: 2001-1371	This strike attempts to access the Oracle 9i Soap Router interface. This interface does not enforce authentication in the default configuration.
Strike Oracle 9i HTTP Server Web Administration Access	BID: 4292  CVE: 2002-0561	This strike attempts to access the Oracle 9i web administration interface in a way that bypasses the authentication phase.
Strike Oracle 9i HTTP Server XSQLServlet XSQLConfig.xml Access	BID: 4290  CVE: 2002-0568	This strike attempts to access the Oracle 9i XSQLServlet configuration file.
Strike Apache Stronghold Server Information Disclosure		This strike attempts to access the Apache Stronghold stronghold-info page.
Strike Apache Stronghold Server Status Disclosure		This strike attempts to access the Apache Stronghold stronghold-status page.
Strike Sensitive File Access .svn-entries		This strike attempts to access a Subversion entries file in the web root.
Strike Apache System User Directory Access bin		This strike attempts to access a system user's web directory over HTTP.
Strike Apache System User Directory Access cron		This strike attempts to access a system user's web directory over HTTP.
Strike Apache System User Directory Access root		This strike attempts to access a system user's web directory over HTTP.
Strike Sensitive File Access ws_ftp.log		This strike attempts to access a WS_FTP transfer log file.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Sensitive File Access WS_FTP.LOG		This strike attempts to access a WS_FTP transfer log file.
Strike Apache File Access .www_acl		This strike attempts to access an Apache configuration file over HTTP.
Strike Apache File Access .wwwacl		This strike attempts to access an Apache configuration file over HTTP.
Strike Apache File Access .wwwgroup		This strike attempts to access an Apache configuration file over HTTP.
Strike Apache File Access .wwwpasswd		This strike attempts to access an Apache configuration file over HTTP.
Strike ACGVclick function.inc.php path Parameter PHP File Include	CVE: 2007-0577  BID: 22278	This strike exploits a PHP include flaw in the ACGVclick web application.
Strike Adobe Acrobat Reader getIcon Memory Corruption (HTTP)	BID: 34169  CWE: 20  CVE: 2009-0927	This strike exploits a flaw in Adobe's PDF reader that can result in the execution of arbitrary code.
Strike Actionpoll index.php include Parameter PHP File Include	CVE: 2001-1296  BID: 3383	This strike exploits a PHP include flaw in the Actionpoll PHP voting application.
Strike Actionpoll index.php include_dir Parameter PHP File Include	CVE: 2001-1296  BID: 3383	This strike exploits a PHP include flaw in the Actionpoll PHP voting application.
Strike Active Calendar 1.2 showcode.php page Parameter Local File Include	CVE: 2007-1110  BID: 22704	This strike exploits a local file include vulnerability in Active Calendar 1.2
Strike Active Calendar 1.2 flatevents.php css Parameter XSS	BID: 22705  CVE: 2007-1111	This strike exploits a cross-site scripting vulnerability in Active Calendar 1.2

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Active Calendar 1.2 mysqlevents.php css Parameter XSS	BID: 22705 CVE: 2007-1111	This strike exploits a cross-site scripting vulnerability in Active Calendar 1.2
Strike Active Calendar 1.2 m_4.php css Parameter XSS	BID: 22705 CVE: 2007-1111	This strike exploits a cross-site scripting vulnerability in Active Calendar 1.2
Strike ActiveCampaign 1-2- All Admin Panel Username Parameter SQL Injection	BID: 15400 CVE: 2005-3679	This strike exploits a SQL injection flaw in the ActiveCampaign 1-2-All web application.
Strike ActiveCampaign 1-2- All main.php username Parameter SQL Injection	CVE: 2005-3679 BID: 15400	This strike exploits a SQL injection vulnerability in the username field of 1-2-All
Strike ActivePerl perlIS.dll Filename Overflow Variant 1	CVE: 2001-0815 BID: 3526	This strike exploits a buffer overflow in perlIS.dll in ActivePerl for Microsoft IIS when parsing requests containing a long filename ending in '.pl'.
Strike Activist Mobilization Platform (AMP) base.php base_path Parameter PHP File Include	CVE: 2007-1571	This strike exploits a PHP include flaw in AMP 3.2 and prior.
Strike AdMentor Admin Remote SQL Injection	CVE: 2007-0575 BID: 22281	This strike exploits a remote SQL injection vulnerability in the AdMentor admin page
Strike ADNForum index.php fid Parameter SQL Injection	CWE: 89 CVE: 2006-0123 BID: 16157	This strike exploits a SQL injection flaw in the ADNForum web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Adobe Acrobat AcroPDF.dll loadFile Vulnerability	CVE: 2006-6027 BID: 21155	This strike exploits a memory corruption vulnerability in Adobe Acrobat AcroPDF.dll when passing a long argument to the loadFile method.
Strike Adobe Acrobat AcroPDF.dll setLayoutMode Vulnerability	CVE: 2006-6236 BID: 21813	This strike exploits a memory corruption vulnerability in Adobe Acrobat AcroPDF.dll when passing a long argument to the setLayoutMode() method.
Strike Adobe Acrobat AcroPDF.dll setNamedDest Vulnerability	CVE: 2006-6236 BID: 21813	This strike exploits a memory corruption vulnerability in Adobe Acrobat AcroPDF.dll when passing a long argument to the setNamedDest() method.
Strike Adobe Acrobat AcroPDF.dll setPageMode Vulnerability	CVE: 2006-6236 BID: 21813	This strike exploits a memory corruption vulnerability in Adobe Acrobat AcroPDF.dll when passing a long argument to the setPageMode() method.
Strike Adobe Acrobat AcroPDF.dll src Vulnerability	CVE: 2006-6236 BID: 21813	This strike exploits a memory corruption vulnerability in Adobe Acrobat AcroPDF.dll when passing a long argument to the src method.
Strike Adobe Acrobat getAnnots Remote Code Execution (HTTP)	BID: 34736  CWE: 399  CVE: 2009-1492	This strike exploits a code execution vulnerability in Adobe Acrobat Reader.
Strike Adobe Acrobat Reader newPlayer Remote Code Execution (HTTP)	BID: 37331  CWE: 399  CVE: 2009-4324	This strike exploits a code execution vulnerability in Adobe Acrobat Reader's newPlayer() Javascript method.
Strike Adobe Acrobat and Reader Font Parsing Integer Overflow (HTTP)	CWE: 189  CVE: 2010-2862  BID: 42203	This strike exploits improper parsing of embedded fonts with an integer overflow (CoolType.dll) in Adobe Acrobat and Adobe Reader (PDF) documents which results in a denial of service and potential remote code execution.

Name	References	Description
Strike Adobe Flash DefineSceneAndFrameLabelData Tag NULL Pointer Dereference (Wild 1)	CWE: 189 CVE: 2007-0071 BID: 28695	This strike exploits a NULL pointer dereference vulnerability in the Adobe Flash player that is triggered by a DefineSceneAndFrameLabelData tag containing a malformed SceneCount parameter. This particular exploit is based on a sample found in the wild.
Strike Adobe Flash DefineSceneAndFrameLabelData Tag NULL Pointer Dereference (Wild 2)	CWE: 189 CVE: 2007-0071 BID: 28695	This strike exploits a NULL pointer dereference vulnerability in the Adobe Flash player that is triggered by a DefineSceneAndFrameLabelData tag containing a malformed SceneCount parameter. This particular exploit is based on a sample found in the wild.
Strike Adobe Flash plugin Transparent Object Clickjacking Vulnerability	CWE: 264 CVE: 2013-2866	This strike exploits a vulnerability in the Adobe flash plugin for the Google Chrome Browser on Macintosh OSX. The Flash vulnerability exists in the latest version of Chrome and allows for the victim's webcam's audio/video to be hijacked when handling CSS opacity settings that make the window transparent. Normal use of this plugin would prompt the user to allow or deny use to the requesting ip, but in this case it executes without a prompt.
Strike Adobe Flash Player 10.2.153.1 SWF Memory Corruption	CWE: 119 CVE: 2011-0611 BID: 47314	Adobe Flash Player before 10.2.154.27 on Windows, Mac OS X, Linux, and Solaris and 10.2.156.12 and earlier on Android; Adobe AIR before 2.6.19140; and Authplay.dll (aka AuthPlayLib.bundle) in Adobe Reader 9.x before 9.4.4 and 10.x through 10.0.1 on Windows, Adobe Reader 9.x before 9.4.4 and 10.x before 10.0.3 on Mac OS X, and Adobe Acrobat 9.x before 9.4.4 and 10.x before 10.0.3 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted Flash content, object type confusion, ActionScript that adds custom functions to prototypes, and Date objects; and as exploited in the wild in April 2011. This strike delivers an attack consistent with executing arbitrary code in the context of the user logged in with user interaction by way of visiting a malicious webpage.
Strike Adobe Illustrator CS4 .eps Buffer Overflow (HTTP)	CWE: 119 CVE: 2009-4195 BID: 37192	This strike exploits a vulnerability in the way Adobe Illustrator parses Encapsulated Postscript files containing an overly long strings in a DSC comment, causing a buffer overflow and resulting in possible code execution.
Strike Adobe InDesign Server SOAP Script Execution Lack of Authentication	BID: 56574	Adobe InDesign Server contains a lack of authentication vulnerability. SOAP requests are not authenticated. This allows anyone with access to the SOAP port to execute arbitrary scripts.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Adobe Shockwave Director rcsL Chunk Memory Corruption	CWE: 119 CVE: 2010-3653 BID: 44291	This strike exploits an attack on the undocumented rcsL chunk of Shockwave director files in which setting a 4 byte value in a Director file will overwrite EAX with that value and can lead to remote code execution.
Strike Microsoft Internet Explorer ADODB.Connection Denial of Service	CWE: 20 CVE: 2006-5559 BID: 20704	This strike exploits a denial of service flaw in Microsoft Internet Explorer when instantiating calling the Execute() method of the ADODB Activex control.
Strike Windows URI Handling Arbitrary Command Execution (HTTP)	BID: 10889 CVE: 2004-0636	This strike exploits and overflow in the URI handler for AOL Instant Messenger
Strike AINS function.inc.php path Parameter PHP File Include	CVE: 2007-0570 BID: 22259	This strike exploits a PHP include flaw in the AINS web application.
Strike Akarru main_content.php bm_content Parameter PHP File Include	CVE: 2006-4645 BID: 19870	This strike exploits a PHP include flaw in the Akarru social bookmarking web application.
Strike AlienVault USM and OSSIM fqdn Command Injection	EXPLOITDB : 41884	This strike exploits a command injection vulnerability in the network component of AlienVault. Specifically, when a POST request is made to the fqdn api the host_ip parameter is not properly validated. It is possible to directly pass a command via the host_ip parameter that will get executed in the shell as the root user.
Strike allCineVid Joomla Component id Parameter SQL Injection Vulnerability	CWE: 89 CVE: 2011-0511 BID: 45840	This strike exploits a SQL injection flaw in the allCineVid 1.0.0 Joomla component.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Altnet Download Manager ActiveX Buffer Overflow	CWE: 119 CVE: 2007-5217 BID: 25903	This strike exploits a buffer overflow vulnerability present in the Altnet Download Manager installed by Kazaa and Grokster. Due to an issue involving improper bounds-checking, a malicious web page can cause the Install function to overflow the buffer, leading to system instability and the possibility of remote code execution.
Strike Android 2.0-2.1 Webkit Use-After-Free Remote Code Execution	CWE: 20 CVE: 2010-1807 BID: 43047	This strike exploits a remote code execution vulnerability in WebKit. The flaw occurs when handling floating point data. Remote attacker can use this vulnerability do to code execution on the target system.
Strike Andys PHP KnowledgeBase a_viewusers.php Parameter SQL Injection	CWE: 89 CVE: 2011-1546 BID: 47097	This strike exploits a SQL injection flaw in Andy's PHP KnowledgeBase web application.
Strike AnnoncesV annonce.php page Parameter PHP File Include Variant 1	CVE: 2006-4622 BID: 19854	This strike exploits a PHP include flaw in the AnnonceV web application.
Strike AnnoncesV annonce.php page Parameter PHP File Include Variant 2	CVE: 2006-4622 BID: 19854	This strike exploits a PHP include flaw in the AnnonceV web application.
Strike Anzeigenmarkt 2011 index.php Parameter SQL Injection	CWE: 89 CVE: 2011-1667 BID: 47136	This strike exploits a SQL injection flaw in Anzeigenmarkt 2011 web application.
Strike AOL 9.5 ActiveX AppContext Buffer Overflow		This strike exploits a buffer overflow in an AOL 9.5 ActiveX control when calling the AppContext function.
Strike AOL 9.5 ActiveX DisplayName Buffer Overflow	CWE: 119 CVE: 2007-6699 BID: 27026	This strike exploits a buffer overflow in an AOL 9.5 ActiveX control when calling the DisplayName function.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike AOL 9.5 ActiveX FinalSavePath Buffer Overflow	CWE: 119 CVE: 2007-6699 BID: 27026	This strike exploits a buffer overflow in an AOL 9.5 ActiveX control when calling the FinalSavePath function.
Strike AOL 9.5 ActiveX ForceSaveTo Buffer Overflow	CWE: 119 CVE: 2007-6699 BID: 27026	This strike exploits a buffer overflow in an AOL 9.5 ActiveX control when calling the ForceSaveTo function.
Strike AOL 9.5 ActiveX HiddenControls Buffer Overflow	CWE: 119 CVE: 2007-6699 BID: 27026	This strike exploits a buffer overflow in an AOL 9.5 ActiveX control when calling the HiddenControls function.
Strike AOL 9.5 ActiveX InitialEditorScreen Buffer Overflow	CWE: 119 CVE: 2007-6699 BID: 27026	This strike exploits a buffer overflow in an AOL 9.5 ActiveX control when calling the InitialEditorScreen function.
Strike AOL 9.5 ActiveX Locale Buffer Overflow	CWE: 119 CVE: 2007-6699 BID: 27026	This strike exploits a buffer overflow in an AOL 9.5 ActiveX control when calling the Locale function.
Strike AOL 9.5 ActiveX Proxy Buffer Overflow	CWE: 119 CVE: 2007-6699 BID: 27026	This strike exploits a buffer overflow in an AOL 9.5 ActiveX control when calling the Proxy function.
Strike AOL 9.5 ActiveX SoapURL Buffer Overflow		This strike exploits a buffer overflow in an AOL 9.5 ActiveX control when calling the SoapURL function.

Name	References	Description
Strike AOL 9.5 ActiveX UserAgent Buffer Overflow	CWE: 119 CVE: 2007-6699 BID: 27026	This strike exploits a buffer overflow in an AOL 9.5 ActiveX control when calling the UserAgent function.
Strike Apache APR_PSPrintf Memory Corruption Vulnerability	CVE: 2003-0245 BID: 7723	This strike exploits a buffer overflow flaw in the Apache HTTP server.
Strike Apache apr-util IPv6 URI Parsing Buffer Overflow 1	CVE: 2004-0786	This strike exploits a vulnerability in the way Apache 2.0.35 - 2.0.50 parses IPv6 URI addresses. An attacker can request a malformed literal address which causes a buffer overflow and could potentially lead to code execution.
Strike Apache apr-util IPv6 URI Parsing Buffer Overflow 2	CVE: 2004-0786	This strike exploits a vulnerability in the way Apache 2.0.35 - 2.0.50 parses IPv6 URI addresses. An attacker can request a malformed literal address which causes a buffer overflow and could potentially lead to code execution.
Strike Apache apr-util IPv6 URI Parsing Buffer Overflow 3	CVE: 2004-0786	This strike exploits a vulnerability in the way Apache 2.0.35 - 2.0.50 parses IPv6 URI addresses. An attacker can request a malformed literal address which causes a buffer overflow and could potentially lead to code execution.
Strike Apache auth_ldap Username Format String	CWE: 134 CVE: 2006-0150 BID: 16177	This strike exploits a format string vulnerability in the Apache webserver auth_ldap module. This strike sends a HTTP basic authorization header that contains a username with format specifier characters and a blank password.
Strike Apache Chunked Encoding Overflow - Apache Nosejob	CVE: 2002-0392 BID: 5033	This strike exploits a buffer overflow flaw in the Apache HTTP server. This strike is based on the nosejob.c proof-of-concept exploit.
Strike Apache Chunked Encoding Overflow - Apache Nosejob (Evade)	CVE: 2002-0392 BID: 5033	This strike exploits a buffer overflow flaw in the Apache HTTP server. This strike is based on the nosejob.c proof-of-concept exploit.
Strike Apache Chunked Encoding Overflow - Apache Scalp	CVE: 2002-0392 BID: 5033	This strike exploits a buffer overflow flaw in the Apache HTTP server. This strike is based on the scalp.c proof-of-concept exploit.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Apache Chunked Encoding Overflow - Apache Scalp (Evade)	CVE: 2002-0392 BID: 5033	This strike exploits a buffer overflow flaw in the Apache HTTP server. This strike is based on the scalp.c proof-of-concept exploit.
Strike Apache Continuum Remote Code Execution	EXPLOITDB : 39945	This strike exploits a vulnerability in Apache Continuum. Specifically in versions 1.4.2 and prior, due to the lack of sanitization of user input, it is possible to inject code into the installation.varValue parameter of an HTTP request to the continuum/saveInstallation.action URI. This type of code injection can lead to remote code execution on the target system.
Strike Apache httpd Range Header Memory Exhaustion Denial Of Service	CWE: 399 CVE: 2011-3192 BID: 49303	This strike exploits a denial of service bug in the processing of long range lists in the Apache Web Server. This flaw causes system resource consumption and could lead to instability and denial of service.
Strike Apache Solr Velocity-template Code Execution	EXPLOITDB : 47572 CVE: 2019-17558 CWE: 74	This strike exploits a remote code execution in Apache Solr via Velocity template in the VelocityResponseWriter plugin. When params resource loader is set to true, the user will be allowed to specify the loading of related resources by setting the parameters in the request, this allows the attacker to construct a threatening request on the server. Successful exploitation will result in code execution, in the context of the user running the Apache Solr service.
Strike Apache Struts2 2.1 OGNL Remote Code Execution	BID: 41592 CVE: 2010-1870	This strike exploits a vulnerability present in Apache Struts2 2.1 where a user can encode restricted characters in order to bypass protections put in place to prevent method execution.
Strike Apache Struts2 code execution	CWE: 732 CVE: 2011-3923 BID: 51628	The strike exploits a malicious code execution vulnerability present in apache struts2. The attacker can execute command by sending crafted HTTP request.
Strike Apache Tomcat Hash Collision Denial Of Service	CWE: 399 CVE: 2011-4858 BID: 51200	This strike exploits a denial of service bug in Apache Tomcat when parameters have the same internal hash.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Apache Win32 DOS Batch File Arbitrary Command Execution	CVE: 2002-0061 BID: 4335	This strike exploits a remote command execution flaw in the Apache HTTP server. It attempts to run a random command and pipe the results to a file.
Strike Apple Safari PubSubAgent libxml2 Longentity Memory Corruption	CWE: 119 CVE: 2008-3529 BID: 31126	This strike triggers a heap memory corruption vulnerability in Apple Safari PubSubAgent due to the mishandling of long XML entity names by libxml2.
Strike Apple Quicktime for Windows QTPlugin.ocx ActiveX Control SetBgColor Denial of Service	CWE: 119 CVE: 2008-0778 BID: 27769	This strike exploits a denial of service vulnerability in the QTPlugin.ocx Activex control when calling the SetBgColor method.
Strike Apple Quicktime for Windows QTPlugin.ocx ActiveX Control SetHREF Denial of Service	CWE: 119 CVE: 2008-0778 BID: 27769	This strike exploits a denial of service vulnerability in the QTPlugin.ocx Activex control when calling the SetHREF method.
Strike Apple Quicktime for Windows QTPlugin.ocx ActiveX Control SetMatrix Denial of Service	CWE: 119 CVE: 2008-0778 BID: 27769	This strike exploits a denial of service vulnerability in the QTPlugin.ocx Activex control when calling the SetMatrix method.
Strike Apple Quicktime for Windows QTPlugin.ocx ActiveX Control SetMovieName Denial of Service	CWE: 119 CVE: 2008-0778 BID: 27769	This strike exploits a denial of service vulnerability in the QTPlugin.ocx Activex control when calling the SetMovieName method.
Strike Apple Quicktime for Windows QTPlugin.ocx ActiveX Control SetTarget Denial of Service	CWE: 119 CVE: 2008-0778 BID: 27769	This strike exploits a denial of service vulnerability in the QTPlugin.ocx Activex control when calling the SetTarget method.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Apple Safari 4.0.4 & Google Chrome 4.0.249 CSS Style Stack Overflow		This strike exploits a denial of service vulnerability in Apple Safari 4.0.4 and Google Chrome 4.0.249 when wrapping an extremely long string inside of a CSS style tag.
Strike Apple Safari Javascript Multibyte Character Escaping DoS		This strike triggers a denial of service in the Apple Safari web browser when handling Javascript that escapes multibyte character strings.
Strike Apple Safari KWQListIteratorImpl () HTML Tag Handling DoS	CVE: 2006-1986 BID: 17634	This strike exploits a denial of service flaw in the Apple Safari web browser.
Strike Apple Safari objc_msgSend_rtp() HTML Tag Handling DoS	CVE: 2006-1987 BID: 17634	This strike exploits a denial of service flaw in the Apple Safari web browser.
Strike Apple Safari for Windows Beta feed --URL DoS Variant 1	BID: 24460	This strike exploits a denial of service flaw in Apple Safari for Windows Beta. This flaw is triggered when the browser attempts to open feed:// urls with special characters.
Strike Apple Safari for Windows file -- URL Denial of Service	CWE: 119 CVE: 2008-2001	This strike exploits a denial of service vulnerability in Apple Safari for Windows when attempting to download a file with a crafted URL.
Strike Apple Safari for Windows document.write Denial of Service	CWE: 119 CVE: 2008-2001	This strike exploits a denial of service vulnerability in Apple Safari for Windows when calling document.write in an infinite loop.
Strike Apple Safari 3.0 for Windows IFRAME SRC Shell Metacharacter Command Execution	CWE: 264 CVE: 2007-3186 BID: 24434	This strike exploits a vulnerability in Apple's Safari browser for Windows by passing shell metacharacters in the SRC attribute of an IFRAME tag using a gopher:// uri.
Strike Apple Safari for Windows URL Spoofing	CVE: 2008-1999	This strike exploits a URL spoofing vulnerability in Apple Safari for Windows and Mac OS X when displaying a page with a crafted URL.

Name	References	Description
Strike Apple Webkit HTML Parsing Rowspan Denial of Service	CWE: 399  CVE: 2007-0342  BID: 22059	This strike exploits a denial of service vulnerability in Apple Webkit when parsing HTML with a large ROWSPAN HTML attribute.
Strike APT-29 Sep 2020 Campaign - WellMess Command and Control		This strike simulates the 'APT-29 Sep 2020 Campaign - WellMess Command and Control' traffic that occurs after executing the WellMess malware.
Strike Arcserve Unified Data Protection EdgeServiceImpl Information Disclosure	CWE: 200  CVE: 2015-4069  BID: 74838	This strike exploits an information disclosure vulnerability in Arcserve Unified Data Protection version 5.0 update 3. The vulnerability is caused by improper validation of user authorization when sending SOAP requests to the EdgeServiceImpl getBackupPolicy and getBackupPolicies methods. A remote, unauthenticated attacker could exploit this by sending crafted requests to the service, resulting in the disclosure of sensitive information such as passwords or encryption keys.
Strike Microsoft IIS ASP Chunked Encoding Heap Overflow	CVE: 2002-0079  BID: 4485	This strike exploits a heap overflow flaw in the chunked encoding transfer mechanism in Microsoft IIS ASP.
Strike ASP.NET Hash Collision Denial Of Service	CWE: 399  CVE: 2011-3414	This strike exploits a denial of service bug in ASP.NET when parameters have the same internal hash.
Strike AssetMan download_pdf.php pdf_file Parameter Directory Traversal	BID: 22921  CVE: 2007-1427	This strike exploits a directory traversal vulnerability in AssetMan
Strike Digium Asterisk Management Interface HTTP Digest Authentication Stack Buffer Overflow	CWE: 119  CVE: 2012-1184  BID: 52815	This strike exploits a buffer overflow vulnerability in the Auth Digest field of the Digium Asterisk Web Management Interface.
Strike Atmosphere Java Framework Reflected Cross Site Scripting		This strike exploits a reflected cross site scripting vulnerability in Atmosphere Java Framework. The vulnerability resides in the JSONP transport method supported by the framework and is due to insufficient sanitization. By exploiting this flaw, an attacker obtains client-side Javascript code execution within victim's browser which can lead to information disclosure and credentials theft.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike AWStats awstats.pl configdir Parameter Command Execution	BID: 12298 CWE: 20 CVE: 2005-0116	This strike exploits an arbitrary command execution flaw the AWStats CGI application.
Strike AWStats rawlog Plugin File Disclosure	BID: 10950 CVE: 2005-0435	This strike exploits a file disclosure flaw the AWStats CGI application.
Strike Axis SSI anonymous view RCE	EXPLOITDB : 43984	This strike exploits a command injection vulnerability in Axis SSI camera. If the camera is configured to allow anonymous view, a remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the server. A successful attack may result in arbitrary command execution or arbitrary file read.
Strike Barracuda IMG.PL f Parameter Command Execution	BID: 14712 CVE: 2005-2847	This strike exploits an arbitrary command execution flaw the Barracuda CGI application.
Strike Beautifier Core.php BEAUT_PATH Parameter PHP File Include	CVE: 2006-4044 BID: 19873	This strike exploits a PHP include flaw in the Beautifier web application.
Strike Belkin Wemo ChangeFriendlyName XSS	CWE: 79	This strike exploits an XSS code injection vulnerability in the Belkin Wemo application. Specifically it is possible for an attacker to inject code into the ChangeFriendlyName parameter when sending a POST request to the listening basicevent1 service of the Belkin application. The attacker can potentially use this vulnerability to perform various functions like exfiltrating images and GPS tracking, because the Wemo application has been granted access to these services.
Strike Bharat Mediratta Gallery index.php include Parameter PHP File Include	CVE: 2001-1234 BID: 3397	This strike exploits a PHP include flaw in the Bharat Mediratta Gallery.
Strike Bharat Mediratta Gallery index.php include_dir Parameter PHP File Include	CVE: 2001-1234 BID: 3397	This strike exploits a PHP include flaw in the Bharat Mediratta Gallery.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Bharat Mediratta Gallery captionator.php GALLERY_BASEDIR Parameter PHP File Include	CVE: 2002-1412 BID: 5375	This strike exploits a PHP include flaw in the Bharat Mediratta Gallery.
Strike Cross Site Request Forgery Vulnerability in ManageEngine EventLog Analyzer	BID: 74743	This strike exploits a cross site request forgery vulnerability inside ManageEngine EventLog Analyzer. The vulnerability is due to improper userManagementForm.do input validation. An attacker could exploit this vulnerability in order submit requests on the target system with valid user privileges.
Strike Oracle Business Transaction Management SOAP DeleteFileRequest Arbitrary File Deletion	BID: 54870	This strike exploits an arbitrary file deletion vulnerability in Oracle Business Transaction Management Server. A specially crafted SOAP request can be used to delete arbitrary files with System privileges, including system critical files. Successful exploitation can result in data loss or a denial of service condition.
Strike Sinapsi eSolar Light Photovoltaic System Monitor SQL Injection	BID: 55872  CWE: 89  CVE: 2012-5861	This strike exploits SQL injection vulnerabilities in Sinapsi eSolar Light Photovoltaic System Monitor.
Strike Siemens Solid Edge WebPartHelper ActiveX Remote Code Execution Vulnerability	BID: 60158	This strike exploits a remote code-execution vulnerability in SIEMENS Solid Edge. The vulnerability is due to the use of OpenInEditor method within the WebPartHelper ActiveX Control. By enticing a user to open a crafted web page an attacker could remotely execute arbitrary code.
Strike Bit 5 Blog processlogin.php username Parameter SQL Injection	CVE: 2006-0320  BID: 16244	This strike exploits a SQL injection flaw in the Bit 5 Blog web application.
Strike B-net Software Content Management System shout.php name Parameter XSS	CVE: 2006-0078  BID: 16114	This strike exploits a cross site scripting flaw in the B-net Software Content Management System.
Strike Boite de News index.php url_index Parameter PHP File Include	CVE: 2006-4123  BID: 19440	This strike exploits a PHP remote file include flaw in the Boite de News web application.
Strike Microsoft Internet Explorer Frameset Null Pointer Dereference		This strike exploits a Denial of Service in Microsoft Internet Explorer. The vulnerability is triggered when a specific HTML element attribute is set to an unallowed value. By enticing a user to view a malicious web page, an attacker can cause the vulnerable browser to crash. NOTE: The vendor does not intend to issue a patch for this vulnerability.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike CA BrightStor ARCserve Backup r11.5 ActiveX AddColumn Buffer Overflow	CWE: 119 CVE: 2008-1472 BID: 28268	This strike exploits flaw in an ActiveX control that ships with CA Brightstor ARCserve Backup r11.5 that can be triggered by sending an overly long string as the first argument to the AddColumn method resulting in a buffer overflow and potentially leading to arbitrary code execution.
Strike Centreon Web Interface UserAlias Command Execution	EXPLOITDB : 40170	This strike exploits a vulnerability in Centreon Web Interface. The vulnerability is due to how Centreon utilizes the echo command for logging SQL errors. It is possible for an unauthenticated attacker to abuse this functionality to inject and execute commands remotely at the login screen.
Strike CHETCPASSWD System Shadow File Disclosure	CVE: 2002-2219 BID: 6472	This strike exploits a flaw in CHETCPASSWD that discloses the tail end of the system shadow file
Strike Chimera Web Portal System linkcategory.php id Parameter SQL Injection	CVE: 2006-0137 BID: 16113	This strike exploits a SQL injection flaw in the Chimera Web Portal Application.
Strike Chimera Web Portal System modules.php comment_poster Parameter XSS	CVE: 2006-0136 BID: 16113	This strike exploits multiple cross site scripting flaws in the Chimera Web Portal Application.
Strike Chimera Web Portal System modules.php comment_poster_email Parameter XSS	CVE: 2006-0136 BID: 16113	This strike exploits multiple cross site scripting flaws in the Chimera Web Portal Application.
Strike Chimera Web Portal System modules.php comment_text Parameter XSS	CVE: 2006-0136 BID: 16113	This strike exploits multiple cross site scripting flaws in the Chimera Web Portal Application.
Strike Chipmunk Guestbook addentry.php homepage Parameter XSS	CVE: 2006-0069 BID: 16112	This strike exploits a cross site scripting flaw in the Chipmunk Guestbook.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Google Chrome PDF Viewer Use-After-Free (HTTP)	BID: 45788 CWE: 399 CVE: 2011-0475	This strike exploits a use-after-free vulnerability in Google Chrome before 8.0.552.237 and Google Chrome OS before 8.0.552.344 which causes denial of service conditions and possibly other impact by way of a maliciously crafted PDF file. May require user interaction by way of clicking a form button to exhibit malicious conditions.
Strike Cisco Secure ACS LogonProxy.cgi error Parameter XSS	CVE: 2006-3101 BID: 18449	This strike exploits a cross site scripting flaw in the Cisco Secure ACS LogonProxy.cgi application.
Strike Cisco Secure ACS LogonProxy.cgi SSL Parameter XSS	CVE: 2006-3101 BID: 18449	This strike exploits a cross site scripting flaw in the Cisco Secure ACS LogonProxy.cgi application.
Strike Cisco Secure ACS LogonProxy.cgi Ok Parameter XSS	CVE: 2006-3101 BID: 18449	This strike exploits a cross site scripting flaw in the Cisco Secure ACS LogonProxy.cgi application.
Strike Cisco IOS HTTP Authentication Bypass Level 16	CWE: 287 CVE: 2001-0537 BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 17	CWE: 287 CVE: 2001-0537 BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 18	CWE: 287 CVE: 2001-0537 BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco IOS HTTP Authentication Bypass Level 19	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 20	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 21	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 22	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 23	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 24	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 25	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco IOS HTTP Authentication Bypass Level 26	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 27	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 28	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 29	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 30	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 31	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 32	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco IOS HTTP Authentication Bypass Level 33	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 34	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 35	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 36	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 37	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 38	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 39	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco IOS HTTP Authentication Bypass Level 40	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 41	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 42	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 43	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 44	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 45	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 46	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco IOS HTTP Authentication Bypass Level 47	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 48	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 49	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 50	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 51	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 52	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 53	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco IOS HTTP Authentication Bypass Level 54	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 55	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 56	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 57	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 58	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 59	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 60	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco IOS HTTP Authentication Bypass Level 61	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 62	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 63	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 64	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 65	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 66	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 67	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco IOS HTTP Authentication Bypass Level 68	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 69	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 70	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 71	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 72	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 73	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 74	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco IOS HTTP Authentication Bypass Level 75	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 76	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 77	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 78	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 79	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 80	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 81	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco IOS HTTP Authentication Bypass Level 82	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 83	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 84	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 85	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 86	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 87	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 88	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco IOS HTTP Authentication Bypass Level 89	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 90	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 91	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 92	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 93	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 94	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 95	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco IOS HTTP Authentication Bypass Level 96	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 97	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 98	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco IOS HTTP Authentication Bypass Level 99	CWE: 287  CVE: 2001-0537  BID: 2936	This strike attempts to execute arbitrary IOS commands through the HTTP interface of a vulnerable router or switch.
Strike Cisco DCP2100 SADownStartingFrequency Denial of Service		This strike exploits a denial of service vulnerability in Cisco DCP2100 devices. A series of HTTP POST commands can be sent to a vulnerable device to remotely restart the router. These commands can be repeatedly sent to create a denial of service condition.
Strike Cisco SA520W Security Appliance Directory Traversal	EXPLOITDB : 44650	The vulnerability allows attackers read access to arbitrary file contents accessible in the Cisco SA520W Security Appliance server by insufficient validation of user input on requests. Successful exploitation could result in arbitrary file access on the target server.
Strike Cisco WebEx UCF atucfobj.dll ActiveX NewObject Buffer Overflow	CWE: 119  CVE: 2008-3558  BID: 30578	There exists a stack-based buffer overflow in the WebexUCFObject ActiveX control in atucfobj.dll in Cisco WebEx Meeting Manager before 20.2008.2606.4919 which allows remote attackers to execute arbitrary code via a long argument to the NewObject method. This strike delivers a payload via an html page that is consistent with triggering the vulnerable conditions of this ActiveX control method buffer overflow flaw.
Strike citrix XML password buffer overflow	BID: 48898	This strike exploits a stack buffer overflow vulnerability in Citrix XenApp and XenDesktop via XML service.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike citrix XML service request memory corruption	BID: 48898	This strike exploits a memory corruption vulnerability in Citrix XenApp and XenDesktop via XML service. The vulnerability is due to lack of input sanitation. Remote attacker could take advantage of this vulnerability to do code execution attack on the target system.
Strike Clipbucket Arbitrary PHP Code Execution		This strike exploits a file upload vulnerability in Clipbucket web application. The vulnerability is due to improper validation of the user controlled input to the file uploading scripts. By exploiting this vulnerability, a remote, unauthenticated attacker can upload any file including PHP scripts and execute them on the target server. NOTE: When run in one-arm mode, target web application index needs to be available at http://[server].
Strike Clipbucket - Operating System Command Injection		This strike exploits a command injection vulnerability in Clipbucket web application. The vulnerability is due to improper input validation of the "file_name" parameter in HTTP requests to "file_uploader.php" script. By exploiting this vulnerability, a remote, unauthenticated attacker can execute arbitrary OS commands on the target server. NOTE: When run in one-arm mode, file_uploader.php script needs to be available at http://[server]/api/file_uploader.php. Test will create a file named "exploited" in the same location as the vulnerable script.
Strike Code Avalanche inc_listnews.asp CAT ID Parameter SQL Injection	CVE: 2007-1021 BID: 22582	This strike exploits an SQL injection vulnerability in Code Avalanche
Strike Comet WebFileManager CheckUpload.php Language Parameter PHP File Include	CVE: 2006-4077 BID: 19433	This strike exploits a PHP include flaw in the Comet WebFileManager. The checkupload.php script does not properly sanitize the Language variable before use.
Strike CommuniCrypt ActiveX Control Buffer Overflow		This strike exploits a buffer overflow vulnerability inside the CommuniCrypt ActiveX control. If an overly long string is passed to the AddAttachments method a buffer will overflow.
Strike Coppermine Blind SQL Injection	CVE: 2007-1107 BID: 22709	This strike exploits a blind SQL injection vulnerability in the Coppermine Photo Gallery
Strike cPanel 9.1.0-R85 testfile.html email Parameter XSS	BID: 10002  CWE: 79  CVE: 2004-1875	This strike exploits a cross-site scripting vulnerability in the cPanel remote administration package

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike cPanel 9.1.0-R85 erredit.html file Parameter XSS	BID: 10002  CWE: 79  CVE: 2004-1875	This strike exploits a cross-site scripting vulnerability in the cPanel remote administration package
Strike cPanel 9.1.0-R85 dnslook dns Parameter XSS	BID: 10002  CWE: 79  CVE: 2004-1875	This strike exploits a cross-site scripting vulnerability in the cPanel remote administration package
Strike cPanel 9.1.0-R85 ignorelist.html account Parameter XSS	BID: 10002  CWE: 79  CVE: 2004-1875	This strike exploits a cross-site scripting vulnerability in the cPanel remote administration package
Strike cPanel 9.1.0-R85 showlog.html account Parameter XSS	BID: 10002  CWE: 79  CVE: 2004-1875	This strike exploits a cross-site scripting vulnerability in the cPanel remote administration package
Strike cPanel 9.1.0-R85 repairdb.html db Parameter XSS	BID: 10002  CWE: 79  CVE: 2004-1875	This strike exploits a cross-site scripting vulnerability in the cPanel remote administration package
Strike cPanel 9.1.0-R85 doaddftp.html login Parameter XSS	BID: 10002  CWE: 79  CVE: 2004-1875	This strike exploits a cross-site scripting vulnerability in the cPanel remote administration package
Strike cPanel 9.1.0-R85 editmsg.html account Parameter XSS	BID: 10002  CWE: 79  CVE: 2004-1875	This strike exploits a cross-site scripting vulnerability in the cPanel remote administration package

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike cPanel 9.1.0-R85 del.html ip Parameter XSS	BID: 10002 CWE: 79 CVE: 2004-1875	This strike exploits a cross-site scripting vulnerability in the cPanel remote administration package
Strike CS Chat-r-box csChatRBox.cgi setup Parameter Code Execution	CVE: 2002-1752 BID: 4452	This strike exploits an arbitrary code execution flaw in the csChatRBox website chat application.
Strike CSGuestbook csGuestbook.cgi setup Parameter Code Execution	CVE: 2002-1750 BID: 4448	This strike exploits an arbitrary code execution flaw in the csGuestbook website guestbook application.
Strike CSLiveSupport csLiveSupport.cgi setup Parameter Code Execution	CVE: 2002-1751 BID: 4450	This strike exploits an arbitrary code execution flaw in the csLiveSupport website client support application.
Strike CSNews csNews.cgi setup Parameter Code Execution	CVE: 2002-1751 BID: 4450	This strike exploits an arbitrary code execution flaw in the csNews website news management application.
Strike csSearch csSearch.cgi Arbitrary Command Execution	CVE: 2002-0495 BID: 4368	This strike exploits an arbitrary code execution flaw in the csSearch website search application.
Strike Microsoft Internet Explorer mergeAttribues Property Handling Memory Corruption	CVE: 2007-0945 BID: 23769	Microsoft Internet Explorer contains a memory corruption vulnerability. The mergeAttribues method will copy the attributes, events, and styles from one DOM object to another without validating the type of object passed in. If attributes exist in the source object which do not exist in the destination object, those attributes may write in out-of-bounds memory, resulting in memory corruption. Successful exploitation may result in arbitrary code execution with user privileges or abnormal termination of Internet Explorer.
Strike Microsoft Internet Explorer cloneNode Dereferenced Pointer Memory Corruption	CWE: 399 CVE: 2007-3903 BID: 26816	Microsoft Internet Explorer contains a memory corruption vulnerability. If an element object is created with no variable referencing it, the memory will be freed during garbage collection. If cloneNode is then called on that object, which contains a pointer to the now freed memory, memory corruption could occur. Successful exploitation could lead to execution of arbitrary code or abnormal termination of Internet Explorer.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Ask.com Toolbar activeX Control Buffer Overflow	CWE: 119 CVE: 2007-5107 BID: 25785	This strike identifies a stack buffer overflow in Ask.com Toolbar 4.0.2.53. When passing an overly long string argument to the ShortFormat method of the vulnerable control a stack buffer overflows.
Strike Icona SpA C6 Messenger ActiveX Control File Download and Execute	CWE: 264 CVE: 2008-2551 BID: 29519	This strike executes a vulnerability in Icona SpA C6 Messenger. When the DownloaderActiveX Control propPostDownloadAction parameter is set to run, a remote attacker can download and execute a file via a URL in propDownloadUrl parameter. This strike sends the initial html that contains these parameters before they make an outbound request to receive a malicious file via the propDownloadUrl parameter.
Strike Symantec appstream launchobj ActiveX code execution	CWE: 20 CVE: 2008-4388 BID: 33247	This strike exploits a Symantec appstream client launchobj ActiveX control code execution vulnerability which is due to no confirmation when executing the command in the ActiveX control. Remote attackers may do arbitrary file creation on the target system.
Strike HP Openview Network Node Manager ovlaunch HTTP Request Buffer Overflow	CWE: 119 CVE: 2008-4562 BID: 33668	This strike exploits a buffer overflow vulnerability in HP OpenView Network Node Manager (NMM). The vulnerability is due to insufficient validation of user-supplied data. By sending a specially crafted HTTP request an unauthenticated attacker could potentially execute arbitrary code on the target server.
Strike Free Download Manager torrent File String Buffer Overflow	CWE: 119 CVE: 2009-0184 BID: 33555 EXPLOITDB : 16634	This strike exploits a stack buffer overflow vulnerability in Free Download Manager. Multiple vulnerabilities can be triggered by use of overly long string values. By enticing a user to open a malicious file with the affected software, an attacker could execute arbitrary code.
Strike Orbit Downloader URL Parameter Buffer Overflow	CWE: 119 CVE: 2009-0187 BID: 33894	This strike exploits a buffer overflow vulnerability in Orbit Downloader. Due to improper validation, if a string greater than 472 bytes is passed to the host field in the URL string a stack buffer will overflow.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Novell eDirectory iMonitor HTTP Header Buffer Overflow	BID: 33928 BID: 35666 CWE: 189 CVE: 2009-0192	This strike identifies a vulnerability that exists in Novell eDirectory's iMonitor. Specifically when handling HTTP requests, the Accept-language header is not properly validated, and an overly long string can overflow a buffer causing a denial of service and possibly leading to remote code execution.
Strike Amaya Browser bdo Tag Buffer Overflow	CWE: 119 CVE: 2009-0323 BID: 33046 BID: 33047	This strike exploits a stack overflow vulnerability within Amaya Browser. If an overly long string is sent to the bdo tag the buffer will overflow allowing for the possibility of code execution.
Strike Windows Media Runtime Voice Sample Rate Vulnerability (HTTP)	CWE: 94 CVE: 2009-0555 BID: 36614	This strike exploits a vulnerability parsing the sample rate in ASF-format audio files that use the Windows Media Speech codec
Strike Mozilla Firefox first-letter Memory Corruption	CWE: 399 CVE: 2009-0771 BID: 33990	This strike exploits a Memory Corruption vulnerability in Mozilla Firefox. The vulnerability is due to error while handling svg documents. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.
Strike HP Openview rping buffer overflow	CVE: 2009-1420 BID: 35267	This strike exploits a HP Openview rping buffer overflow vulnerability which is due to bad input check the boundary of the length of hostname. Remote attackers may do arbitrary code execution on the target system.
Strike Novell iPrint Client volatile-date-time parameter Buffer Overflow	BID: 37242 CWE: 119 CVE: 2009-1569	This strike exploits a vulnerability that exists in Novell iPrint Client's ActiveX control ienipp.ocx. When the volatile-date-time parameter is passed to the persistance parameter with a string of more than 61 bytes, a stack buffer is overwritten.
Strike Oracle Secure Backup Administration Authentication Bypass <\>	CVE: 2009-1977 BID: 35672	This strike exploits a authentication bypass inside Oracle's secure backup administration application. The vulnerability resides in the php script that handles authentication and is present due to an input validation error

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle Secure Backup Administration Property Box Command Injection	CVE: 2009-1978 BID: 35678	This strike exploits a command injection vulnerability inside Oracle's Secure Backup Adminstration web interface. The vulnerability allows command injection by passing malicious URL encoded parameters to property_box.php script
Strike Microsoft Internet Explorer Table Layout Corruption	CWE: 94 CVE: 2009-2531	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when a specific nesting of elements is used for a table layout which leads to a memory corruption.
Strike HP Power Manager Server Login variable Buffer Overflow	CWE: 119 CVE: 2009-2685 BID: 36933	This strike exploits a vulnerability in HP Power Manager Server. If an HTP request is sent to the Login URI the code copies the login variable into a fixed stack buffer of 198 bytes. If a larger amount than this is received it will overwrite critical data.
Strike Mozilla Firefox nsPropertyTable Propertylist Memory Corruption	BID: 36343 CVE: 2009-3070	This strike exploits a vulnerability within Mozilla Firefox. PropertyTable::PropertyList dereferences invalid memory and attempts to execute a corrupted function pointer, and if the position is fixed, height is inherit ,and either -moz-column is assigned memory corruption occurs.
Strike Mozilla Products Javascript String Replace Method Buffer Overflow	BID: 36343 CVE: 2009-3075	This strike exploits a vulnerability within Mozilla Firefox and Seamonkey. If the javascript String Replace method is passed both arguments that match the substring, and that string contains a '\$' character, the replace operation is not performed properly. This causes a large string calculation that results in a buffer overflow.
Strike Mozilla Firefox first-letter Pseudo Element Memory Corruption	CVE: 2009-3382 BID: 36866	This strike exploits a Memory Corruption vulnerability in Mozilla Firefox. The vulnerability is due to error while handling first-letter pseudo elements. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.
Strike VMWare Remote Console Format String	CWE: 134 CVE: 2009-3732 BID: 39396	This strike exploits a vulnerability in VMWare's Remote Console program where user controlled values are used for an sprintf call which may include percent modifiers to clobber memory.
Strike HP Openview Network Node Manager ovlogin.exe Buffer Overflow	CWE: 119 CVE: 2009-3846 BID: 37295	This strike exploits a heap buffer overflow vulnerability in HP OpenView Network Node Manager (NMM). The vulnerability is due to insufficient validation of user-supplied data. By sending a specially crafted POST request an unauthenticated attacker could potentially execute arbitrary code on the target server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike HP Openview network node manager buffer overflow	CWE: 119 CVE: 2009-3848 BID: 37296	This strike exploits a HP Openview network node manager buffer overflow vulnerability which is due to bad input check the boundary of the parameter template. Remote attackers may do arbitrary code execution on the target system.
Strike HP OpenView Network Node Manager SNMP OID Buffer Overflow	BID: 37261 BID: 37298 BID: 37299 CWE: 119 CVE: 2009-3849	This strike exploits a vulnerability in HP OpenView's Network Node Manager snmp program. The software does not properly validate or handle code passed to the Oid variable in an HTTP request. If this variable's size is greater than the 4096 byte buffer that is allocated the buffer will be overwritten.
Strike Adobe Download Manager getPlus ActiveX Control Buffer Overflow	CWE: 119 CVE: 2009-3958 BID: 37759	This strike exploits a buffer overflow vulnerability in Adobe Download Manager. The vulnerability is due to a stack-based buffer that can be overflowed by sending one or more overlong strings parameter/name value pairs. Remote attackers could exploit the vulnerability by enticing a user to view a malicious web page.
Strike HP Power Manager Directory Traversal	CWE: 22 CVE: 2009-4000 BID: 37873	This strike exploits a vulnerability in HP's Power manager where a user may use a directory traversal exploit to clobber arbitrary files.
Strike HP Openview user ID and password buffer overflow	CWE: 119 CVE: 2009-4176 BID: 37330	This strike exploits a HP Openview user name and password buffer overflow vulnerability which is due to bad input check the boundary of the length of user name and password. Remote attackers may do arbitrary code execution on the target system.
Strike HP OpenView NNM ovwebsnmpsrv Buffer Overflow	CWE: 119 CVE: 2009-4181 BID: 37343	This strike identifies a vulnerability in the ovwebsnmpsrv.exe service of HP OpenView's Network Node Manager. A buffer overflow exists when parsing the sel value of the request. The number of times this value is copied to a stack buffer of 400 bytes is determined by the OvwSelections parameter in the arg value.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Novell eDirectory dhost stack buffer overflow	CWE: 119 CVE: 2009-4653 BID: 37009 BID: 36815	This strike exploits a Novell eDirectory dhost stack buffer overflow vulnerability which is due to bad input check the length of module name in HTTP request. Remote attackers may do arbitrary code execution on the target system.
Strike Novell eDirectory dhost httpstk password buffer overflow	CWE: 119 CVE: 2009-4654 BID: 37042	This strike exploits a Novell eDirectory dhost httpstk passwords buffer overflow vulnerability which is due to bad input check the length of sadminpwd and verifypwd. Remote attackers may do arbitrary code execution on the target system.
Strike Oracle WebLogic Server Node Manager Command Execution	CVE: 2010-0073 BID: 37926	A command execution vulnerability was found in Oracle WebLogic Server's Node Manager. The vulnerability is due to the fact that the resources of Node Manager utility within WebLogic Server can be reached without authentication. Vulnerability can be exploited by sending a specially crafted HTTP request to the process listening on port 5556/TCP. Successful exploitation can result in arbitrary code execution in the context of the running process.
Strike Symantec IM Manager groupList Parameter SQL Injection	CWE: 89 CVE: 2010-0112 BID: 44299	This strike exploits a SQL injection vulnerability in the groupList parameter in the Symantec IM manager. This vulnerability is due to improper sanitization of an HTTP parameter. A remote attacker could exploit vulnerability to execute arbitrary SQL commands on the target system.
Strike Apache Axis2 Admin Account Default Password	CWE: 255 CVE: 2010-0219 BID: 45625	This strike exploits a vulnerability in several applications. Examples include, but are not limited to, SAP BusinessObjects Enterprise XI 3.2, CA ARCserve D2D r15. The vulnerability is caused by the inclusion of Apache Axis2 with default credentials for the administrator. A remote, unauthenticated attacker could use these credentials to access Axis2 using the admin account, bypassing the application's own security mechanisms. Further on, he would leverage other options (such as file upload) in order to upload a crafted web service file and execute code remotely under the SYSTEM account. The strike is implemented targeting CA ARCserve D2D r15. Post-authentication actions are not simulated as they would largely depend on the attacker's own intentions.
Strike Microsoft Internet Explorer Table Layout Column Corruption	CWE: 94 CVE: 2010-0244 BID: 37891	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when column layouts are modified via code.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer mergeAttributes Method Memory Corruption	CWE: 94 CVE: 2010-0247 BID: 37893	This strike exploits a vulnerability in Microsoft Internet Explorer. The mergeAttributes method is not properly validated, and when an object uses it with the object as the oSource parameter, the attributes are deleted. The object is then called, and because the attributes have been modified, memory corruption will occur.
Strike Microsoft Internet Explorer Microsoft Data Analyzer ActiveX Code Execution	CWE: 94 CVE: 2010-0252	This strike exploits a vulnerability in the Microsoft Data Analyzer ActiveX control. A use after free error while parsing user interface objects allows the remote attacker to execute arbitrary code on the target system.
Strike Microsoft Internet Explorer Mouse Event Uninitialized Memory	BID: 39023 CWE: 94 CVE: 2010-0267	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when referencing mouse events that haven't been properly initialized.
Strike Viscom Software Movie Player Pro ActiveX Control Buffer Overflow	CWE: 119 CVE: 2010-0356	This strike exploits a buffer overflow in Viscom's Movie Player Pro ActiveX control MOVIEPLAYER.MoviePlayerCtrl.1. The strFontName parameter is not properly validated, and if an overly long string is received it will overflow the buffer.
Strike Microsoft Internet Explorer Reference to Incomplete Element	CWE: 94 CVE: 2010-0490 BID: 39031	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when an element is changed which hasn't been completely defined.
Strike Backdoor IBM Cognos Server	CWE: 255 CVE: 2010-0557 BID: 38084	This strike simulates the use of a backdoor account that is hardwired into IBM's Cognos Server.
Strike Microsoft Internet Explorer Rendering Corruption	BID: 39024 CWE: 94 CVE: 2010-0807	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when handling tags that are improperly nested.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle Secure Backup Administration Other Variable Command Injection	CVE: 2010-0899 BID: 41616	This strike exploits a command injection vulnerability inside Oracle's Secure Backup Adminstration web interface. The vulnerability allows command injection by passing malicious URL encoded parameters ("other") to php scripts.
Strike Oracle Secure Backup Administration Authentication Bypass - character	CVE: 2010-0904 BID: 41596	This strike exploits a authentication bypass inside Oracle's secure backup administration application. The vulnerability resides in the php script that handles authentication and is present due to an input validation error
Strike Mozilla Firefox Integer Overflow	CWE: 189 CVE: 2010-1214 BID: 41842	This strike exploits a vulnerability in Mozilla's Firefox where a large number of parameters passed to the Java Runtime Environment leading to a an integer overflow and later to memory corruption.
Strike CA XOsoft multiple Buffer Overflow	CWE: 119 CVE: 2010-1223 BID: 39238	This strike exploits a buffer overflow vulnerability in CA XoSoft production. This vulnerability is due to insufficient boundary checking of parameters while parsing the request. Remote attackers may take advantage of this vulnerability to execute arbitrary code on the target system.
Strike Microsoft Internet Explorer DOM Modification After Release	CWE: 94 CVE: 2010-1259	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when a DOM object is used after it has been released.
Strike Microsoft SharePoint Server Help.aspx Denial of Service	CVE: 2010-1264 BID: 40559	Microsoft Office Sharepoint Services contains a vulnerability in its help.aspx script. By crafting an HTTP request omitting a particular parameter, an attacker can cause a denial of service condition.
Strike RealNetworks Helix Server NTLM Authentication Buffer Overflow	CWE: 119 CVE: 2010-1317 BID: 39490	This strike exploits a vulnerability in RealNetworks Helix Server Products. When handling Base64encoded NTLM Authentication strings of an invalid size, the vulnerable code returns -1 because of a decoding error. This value is then used as a counter to copy data to a heap buffer without validating the error resulting in memory corruption.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Opera Content Length BO	CWE: 189 CVE: 2010-1349 BID: 38519	This strike exploits a buffer overflow vulnerability in Opera 10.10 through 10.50. This vulnerability is due to improper checking content-length value. The attacker can send malicious http response packet with large content-length value lead to buffer overflow.
Strike Safari webkit Remote Code Execution	CWE: 399 CVE: 2010-1392 BID: 40620	This strike exploits a remote code execution vulnerability in Apple Safari. The flaw occurs when handling first-letter attribute in CSS.
Strike Novell iPrint Browser Plugin Buffer Overflow	CWE: 119 CVE: 2010-1527 BID: 42576	This strike exploits a vulnerability that exists in Novell's iPrint Client Browser Plugin. When the call-back-url string is used with op-client-interface-version and result-type set to url, a stack buffer of 200 bytes is allocated for a message string. It is not properly validated, and if an overly long user value is submitted, the buffer is overrun.
Strike HP OpenView Network Node Manager memory Corruption	CWE: 134 CVE: 2010-1550	This strike exploits a vulnerability in HP's OpenView Network Manager where a user-supplied variable is used for a string format which leads to memory corruption.
Strike HP OpenView Network Manager Stack Overflow	CWE: 119 CVE: 2010-1551 BID: 40067	This strike exploits a vulnerability in HP's OpenView Network Manager where a user supplied parameter can overflow a stack buffer.
Strike HP OpenView Network Node Manager act and app Parameter Buffer Overflow	CWE: 119 CVE: 2010-1552	This strike exploits a stack buffer overflow in HP OpenView's Network Node Manager application gennnmdata.exe. A user supplied argument is used to clobber a stack buffer that is a target of sprintf.
Strike HP OpenView Network Node Manager ICount Parameter Buffer Overflow	CWE: 119 CVE: 2010-1554	This strike exploits a stack buffer overflow in HP OpenView's Network Node Manager application gennnmdata.exe. A user supplied argument is used to clobber a stack buffer that is a target of sprintf.

Name	References	Description
Strike HP OpenView Network Node Manager Hostname Overflow	BID: 40072 CWE: 119 CVE: 2010-1555	This strike exploits a vulnerability in HP's OpenView Network Node Manager where a user may supply an overly long hostname to overflow a stack buffer.
Strike VMWare SpringSource Spring Framework class.classloader Code Execution	BID: 40954 CWE: 94 CVE: 2010-1622	This strike exploits a vulnerability in VMWare SpringSource Spring Framework. By abusing the classLoader bean, in a specially crafted request, a remote attacker may achieve arbitrary code execution, by loading a malicious jar file. All versions of SpringSource Spring Framework before 2.5.7 and 3.0.3 are vulnerable to this attack.
Strike Google Chrome Google URL Cross Origin Bypass	CWE: 264 CVE: 2010-1663	This strike exploits a vulnerability within Google's Chrome Browser. Google's URL component does not properly validate URLs that use escape characters, and these characters can allow for insertion of javascript code. In this attack the referenced page's cookie is returned via a javascript alert. With an additional alert from within a body onload event handler the application terminates abruptly.
Strike Apple Quicktime Error Logging Buffer Overflow	CWE: 119 CVE: 2010-1799 BID: 41962	This strike exploits a vulnerability in Apple's Quicktime player when a user controlled string is used to overflow a buffer when logging an error message.
Strike Google Chrome and Apple Safari Webkit Object Outline Memory Corruption	CWE: 119 CVE: 2010-1813 BID: 43078	This strike exploits a vulnerability that exists in Webkit, and is due to the way it handles CSS HTML pages. If the block element contains an inline that has a self painting layer, the code does not check for the correct layer and outlines are mishandled.
Strike Apple Quicktime QTPlugin.ocx plugin invalid pointer	CWE: 824 CVE: 2010-1818	This strike exploits a vulnerability in Apple's Quicktime QTPlugin.ocx plugin where a user supplied pointer is dereferenced without validation.
Strike HP OpenView Network Node Manager Invalid arg	BID: 40637 CWE: 119 CVE: 2010-1960	This strike exploits a stack buffer overflow in HP OpenView's Network Node Manager application jovgraph.exe. A user may supply an overly long argument to a request which clobbers a stack buffer.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike HP OpenView Network Node Manager Sprintf Buffer Overflow	BID: 40638 CWE: 119 CVE: 2010-1961	This strike exploits a stack buffer overflow in HP OpenView's Network Node Manager application jovgraph.exe. A user supplied argument is used to clobber a stack buffer that is a target of sprintf.
Strike Microsoft Internet Explorer Iframe Removal	CWE: 94 CVE: 2010-2556	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when removing an active iframe.
Strike Microsoft Internet Explorer DOM Object Uninitialized Memory Corruption	CWE: 94 CVE: 2010-2557 BID: 42288	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when using the boundElements collection after it has been freed.
Strike Microsoft Internet Explorer Memory Corruption During Layout	CWE: 94 CVE: 2010-2560 BID: 42292	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when trying to adjust layout parameters on a page while it is still being parsed.
Strike Novell Teaming File Upload Directory Traversal	CVE: 2010-2773 BID: 41795	This strike exploits a vulnerability in Novell's Teaming where a user may use a directory traversal exploit to clobber arbitrary files.
Strike Adobe ColdFusion Directory Traversal	CWE: 22 CVE: 2010-2861 BID: 42432	Adobe ColdFusion contains a directory traversal vulnerability. The flaw is due to a lack of input validation by the ColdFusion administration console. A remote unauthenticated attacker could exploit this vulnerability to retrieve arbitrary files, including the password file for the ColdFusion administration console.
Strike Apple CUPS IPP Multiple Value Handling Use After Free	CWE: 399 CVE: 2010-2941 BID: 44530	This strike exploits a use after free vulnerability in Apple Computer Common UNIX Printing System Internet Printing Protocol. When handing certain multi-value parameters with known and unknown strings, memory is not freed properly. This may lead to a use after free condition, which may allow execution of arbitrary code or abnormal termination of the CUPS process.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Squid Proxy Server Expect Empty String Null Pointer Dereference	CVE: 2010-3072 BID: 42982	This strike exploits null pointer dereference vulnerability in Squid Proxy Server. A specially crafted HTTP request with an empty Expect header will trigger a null pointer dereference, leading to abnormal termination of the server process, resulting in a denial of service condition.
Strike Novell iPrint Client debug Parameter Buffer Overflow	CWE: 20 CVE: 2010-3106	This strike exploits a vulnerability that exists in Novell's iPrint Client Browser Plugin. The code does not properly validate the input for the debug parameter. When run, a stack buffer of 0x1FF0 bytes is allocated. If the supplied string is between 0x200 and 0x3FB, a loop will copy more than 1 byte will each iteration through until the stack buffer is overrun and data is overwritten. In this example by triggering the onmousemove event you can slowly watch the buffer fill until it crashes.
Strike Microsoft Internet Explorer Recursive Viewer Corruption of Memory	CWE: 94 CVE: 2010-3326 BID: 43696	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when using a recursively called playStateChange.
Strike Microsoft Internet Explorer Rule Use After Free	CWE: 399 CVE: 2010-3328 BID: 43705	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when removing rules.
Strike Microsoft Internet Explorer Recursive Adding of Elements	CWE: 94 CVE: 2010-3345 BID: 45260	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when recursively adding elements.
Strike Oracle Java Plugin Buffer Overflow	CVE: 2010-3552 BID: 44023	This strike exploits a buffer overflow in Oracle's Java Plugin where a string clobbers a fixed size stack buffer.
Strike Oracle Database Client System Analyzer Arbitrary File Upload	CVE: 2010-3600 BID: 45883	This strike exploits in the Client Analyzer module of Oracle Database 11g. A flaw may allow a remote unauthenticated attacker to upload and execute arbitrary code on vulnerable machine. All version below 11.2.0.1.0 and of Oracle Database 11g and below are vulnerable.

Name	References	Description
Strike RealPlayer CDDA URI Initialization Failure	CWE: 119 CVE: 2010-3747 BID: 44144	This strike exploits an initialization vulnerability within RealNetworks RealPlayer. An overly long string that is passed to the CDDA URI causes an initialization failure, and because this isn't handled properly uninitialized memory is accessed.
Strike Microsoft Unified Access Gateway Cross Site Scripting Vulnerability	CWE: 79 CVE: 2010-3936 BID: 44634	This strike exploits a cross-site scripting vulnerability in Microsoft Forefront Unified Access Gateway (UAG). The vulnerability is due to insufficient validation of user-supplied input in signurl.asp. A remote attacker can exploit this vulnerability by enticing a user to follow a malicious link, which could lead to disclosure of sensitive information, such as web browser authentication cookies or modification of user information.
Strike Microsoft Sharepoint Malformed Request Code Execution Vulnerability	CVE: 2010-3964 BID: 45264	This strike exploits a code execution vulnerability in Microsoft Sharepoint Document Coversion Launcher service. The vulnerability is due to insufficient validation of SOAP requests sent to the service interface. By specially crafting a malicious SOAP request, an unauthenticated attacker could execute arbitrary commands on the server.
Strike IBM Rational Quality Manager Default Account Bypass	CWE: 255 CVE: 2010-4094 BID: 44172	This strike exploits a default credentials vulnerability in IBM Rational Quality Manager. Attacker can use this vulnerability to bypass the authentication on the target system.
Strike HP Power Manager Web Server Stack Overflow	CWE: 119 CVE: 2010-4113	This strike exploits a vulnerability in HP's Power Manager web server where an unauthenticated user can overflow a stack buffer.
Strike Novell ZenWorks Configuration Management File Upload Vulnerability	CWE: 22 CVE: 2010-4229 BID: 47295	This strike exploits a file-upload vulnerability in conjunction with a directory-traversal vulnerability in ZenWorks Configuration Management. These vulnerabilities could allow an unauthenticated attacker to write arbitrary files anywhere on the target system and/or upload and install new web applications. This strike will attempt to upload and install a web application on the target server.
Strike Novell iPrint Client ActiveX control Remote File Deletion	CVE: 2010-4319	This strike exploits a file deletion vulnerability within Novell iPrint Client's ActiveX control. If the CleanupUploadFiles method is called it deletes the files in the zipFilePath parameter without any validation of the parameter. In this attack the folder named removeme will be deleted from C:\.
Strike Oracle GoldenGate Veridata Server XML SOAP Request Buffer Overflow	CVE: 2010-4416 BID: 45868	This strike exploits a buffer overflow vulnerability in the Oracle GoldenGate Veridata Server. The vulnerability is due to failure to properly sanitize user-supplied input data. By crafting an XML SOAP request with an overly long value an attacker could remotely execute arbitrary code on the target server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Mozilla Products SVG Text Container Use After Free Condition	CWE: 94 CVE: 2011-0084	This strike exploits a vulnerability within Mozilla Firefox, Seamonkey, and Thunderbird. When the getCharNumAtPosition method is used with properties of its point argument, it is not validated properly. The getter of the x and y properties removes the same SVGTextContentElement that the method is called on, from DOM tree. When later attempts to access this object are performed a Use after Free condition occurs.
Strike Microsoft Windows MHTML Protocol Handler Cross Site Scripting	CWE: 79 CVE: 2011-0096 BID: 46055	This strike exploits a cross site scripting vulnerability in Microsoft Windows. The mhtml handler does not perform sufficient validation, allowing scripting code to be executed. Successful exploitation may result in execution of arbitrary script code.
Strike HP OpenView Network Node Manager parameter overflow	CWE: 119 CVE: 2011-0267 BID: 45762	This strike exploits a vulnerability in HP's OpenView Network Node Manager where a user may supply a large number of variables that will indirectly clobber a fixed buffer.
Strike HP OpenView nnmRptConfig.exe text1 Buffer Overflow	CWE: 119 CVE: 2011-0268 BID: 45762	This strike exploits a vulnerability in HP OpenView's Network Node Manager Service nnmRptConfig.exe. When the text1 parameter is passed values greater than 0x210 bytes, it overflows a buffer.
Strike HP OpenView nnmRptConfig.exe schd_select1 memory corruption	CWE: 119 CVE: 2011-0269 BID: 45762	This strike exploits a vulnerability in HP OpenView's Network Node Manager Service nnmRptConfig.exe. When the schd_select1 parameter is passed values greater than 0x210 bytes, it overflows a buffer.
Strike InduSoft Thin Client InternationalOrder ActiveX Buffer Overflow	CWE: 119 CVE: 2011-0340 BID: 47596	This strike exploits a vulnerability within InduSoft's Thin Client. If an overly long value is supplied to the International Order Property of the ISSYMBOL.ISSymbolCtrl, then that value is converted to a widechar string, and copied to offset 0x2458 overflowing the buffer.
Strike Apache Stack Overflow Recursion	CWE: 399 CVE: 2011-0419	This strike exploits a recursive call flaw on the Apache server which can lead to stack exhaustion. Even without a crash, the server can be unresponsive for some time.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Symantec IM Manager SQL Injection Vulnerability	CWE: 89 CVE: 2011-0553 BID: 49738	This strike exploits a SQL injection vulnerability in Symantec IM Manager. The vulnerability is due to a failure to properly validate parameters in HTTP requests to IMAdminLDAPConfig.asp. A remote attacker could exploit this vulnerability by enticing an authenticated user to view a malicious web page, resulting in execution of arbitrary SQL code against the IM Manager database.
Strike Symantec IM Manager ProcessAction Remote Code Execution Vulnerability	CWE: 94 CVE: 2011-0554 BID: 49742	This strike exploits a code execution vulnerability in Symantec IM Manager. The vulnerability is due to a lack of input validation of HTTP parameters, specifically rdProcess, by the Management Interface. A remote, unauthenticated attacker can exploit the vulnerability by enticing a user to view a malicious webpage, leading to the execution of arbitrary code contained in an file located on a remote share.
Strike Microsoft SharePoint Calendar Cross Site Scripting Vulnerability	CWE: 79 CVE: 2011-0653 BID: 54316	Microsoft Office Sharepoint contains a cross-site scripting (XSS) vulnerability. The vulnerability is due to insufficient validation of the request URL string by the Sharepoint server. An attacker could entice a user to open a malicious URL which could lead to privilege escalation or information disclosure.
Strike CA Internet Security Suite XMLSecDB Arbitrary File Creation	BID: 46539 CVE: 2011-1036	This strike exploits an arbitrary file creation vulnerability in CA Internet Security Suite XMLSecDB ActiveX control.
Strike IBM Tivoli Endpoint Manager POST Buffer Overflow	CWE: 119 CVE: 2011-1220 BID: 48049	This strike identifies a vulnerability in IBM Tivoli's Endpoint Manager. Specifically the vulnerability occurs when an authenticated POST request is made to vulnerable service lcfd.exe. In this strike we achieve this by utilizing a hardcoded user account (OSVDB 72751) to bypass authentication and proceed with overflowing the buffer by sending a large amount of data in the query.
Strike IBM Rational Rhapsody FlashBack FBRecorder Multiple Vulnerabilities	CWE: 94 CVE: 2011-1388 BID: 51184	This strike exploits multiple vulnerabilities attribute to an ActiveX control of the BB Flashback Recorder. If a user opens a specially crafted web page, on a vulnerable machine, arbitrary file access and memory corruption conditions may be triggered using local privileges. All IBM rational Rhapsody verisions prior to 7.6 as well as Blueberry BB FlashBack SDK FBRecorder prior to 2.0.0.214 are affected.
Strike Webkit before Block Use after Free Condition	CWE: 399 CVE: 2011-1440 BID: 47604	This strike exploits a vulnerability within Apple WebKit. When handling ruby elements within a CSS, if used as a counter and its appearance is modified by a display attribute in the CSS after it is defined in the initial CSS, a use after free condition occurs.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle GlassFish Server Administration security bypass	CVE: 2011-1511 BID: 47818	This strike exploits a security bypass vulnerability in Oracle GlassFish server. The vulnerability is due to improper handling trace request. Attacker can use this vulnerability to bypass the authentication on the target system.
Strike Cisco Unified Communications Manager Multiple SQL Injections	CWE: 89 CVE: 2011-1610	This strike exploits an SQL injection vulnerability in Cisco Unified Communications Manager. The vulnerability arises due to the lack of proper sanitation of user supplied arguments to xmldirectorylist.jsp, xmldirectorylist.utf-8.jsp, and xmldirectorylist.other.jsp. An unauthenticated remote attacker can access the vulnerable web service and inject an SQL query into a parameter, thus allowing an attacker to inject and execute arbitrary SQL commands, which can result in disclosure of sensitive information.
Strike CA Total Defense Suite UnassignFunctionalUsers SQL Injection	CWE: 89 CVE: 2011-1653 BID: 47355	This strike exploits a SQL injection vulnerability within CA Total Defense Suite. This vulnerability is due to improper sanitation of a parameter in UnAssignFunctionalRoles. A remote attacker can take advantage of this vulnerability to inject SQL commands.
Strike CA Total Defense Suite credential disclosure	CWE: 310 CVE: 2011-1655 BID: 47356	This strike exploits a code credential disclosure vulnerability in CA Total Defense Suite product. This vulnerability is due to insufficient checking of the access control. A remote attacker can take advantage of this vulnerability to gain the credential information on the target system.
Strike Microsoft Forefront UAG Default Reflected Cross-site Scripting	BID: 44974 CWE: 79 CVE: 2011-1897	This strike exploits a reflected cross-site scripting (XSS) vulnerability in Microsoft Unified Access Gateway. The vulnerability is caused by improper handling of HTTP query strings. This vulnerability can be exploited by an unauthenticated attacker to elevate privileges, inject arbitrary script code, or spoof an identity on a target system.
Strike Microsoft Report Viewer Cross Site Scripting	CWE: 79 CVE: 2011-1976 BID: 49033	This strike exploits a remote cross-site scripting (XSS) vulnerability in Microsoft Report Viewer. The flaw is due to failure to properly validate input passed to the Microsoft Report Viewer control before returning it to the user. This could allow an attacker to craft a malicious URL that could execute arbitrary script code in the context of the browser.
Strike Microsoft Internet Explorer Scroll Use After Free	CWE: 20 CVE: 2011-1993	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when using a scroll region. A region of memory that had been freed is accessed.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Forefront Unified Access Gateway NULL Cookie	CWE: 20 CVE: 2011-2012 BID: 49980	This strike exploits a vulnerability in Microsoft's Forefront Unified Access Gateway where a cookie can be both defined and NULL which leads to a denial of service.
Strike Cisco AnyConnect Load Previous Software	CWE: 20 CVE: 2011-2039	This strike exploits a flaw in Cisco's AnyConnect software where a previous version of the software may be loaded which contains known vulnerabilities. Then an attacker may use vulnerabilities in that software for an attack. Since the attacker can control the file that is downloaded, any arbitrary file can be delivered.
Strike Tom Sawyer GET Extension Object Initialization Memory Corruption	CWE: 119 CVE: 2011-2217 BID: 48099	This strike exploits a memory corruption vulnerability in a TomSawyer ActiveX controls. If activeX control objects created inside a browser memory corruption occurs because they cannot initialize properly.
Strike Oracle Secure Backup Login Command Injection	CVE: 2011-2261 BID: 48752	This strike exploits a vulnerability in the Oracle Secure Backup server where a user may inject some commands into a login statement which is then executed by the server.
Strike HP Easy Printer Care ActiveX Control Directory Traversal	CWE: 94 CVE: 2011-2404 BID: 49100	HP Easy Printer Care Software contains a directory traversal vulnerability. The flaw is due to a lack of input validation by the SaveXML method. An attacker could exploit this vulnerability to create and/or overwrite files, resulting in a denial of service or remote code execution.
Strike Citrix Access Gateway Plugin for Windows CESC ActiveX Buffer Overflow	CWE: 119 CVE: 2011-2592 BID: 54754	Citrix Access Gateway Plug-in for Windows contains a buffer overflow vulnerability. The length of the CSEC http header is not validated. Successful exploitation can allow execution of arbitrary code with privileges of the current user or abnormal termination of ActiveX.
Strike Novell Zenworks LaunchHelp.dll ActiveX Launch Process Command Execution.xml	CWE: 22 CVE: 2011-2657 BID: 50574	The LaunchHelp.dll ActiveX Control that is included with Novell ZENworks Configuration Management and AdminStudio contains an access control weakness that allows remote code execution via the browser.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Apple Safari and Google Chrome WebKit Float Use After Free	CWE: 399 CVE: 2011-2790	This strike demonstrates a use after free vulnerability in Apple Safari and Google Chrome's Webkit. When the display style of an element changes from a float to a different kind of positioning, the change may not be carried over to the siblings. The parent object tries to free marked siblings, but does not identify them properly and frees incorrect objects.
Strike Apple Safari Webkit Form Tag Denial of Service	CWE: 119 CVE: 2011-2813 BID: 50066	This strike identifies a vulnerability in Apple Safari Webkit. Specifically, when objects that contain the form= attribute are initialized, associated elements are built with pointers to objects containing virtual pointers. When these pointers are referenced later a denial of service condition occurs.
Strike Apple Safari and Google Chrome Webkit DisplayBox Memory Corruption	CWE: 399 CVE: 2011-2818 BID: 48960	This strike demonstrates a vulnerability in Apple Safari and Google Chrome's Webkit. If a flexbox style is used with children of float style, the element does not verify it's style and considers it a float. This returns uninitialized memory.
Strike Citrix Access Gateway SSL VPN Plugin Remote Code Execution	CWE: 119 CVE: 2011-2882	This strike exploits a buffer overflow in Citrix's Access Gateway SSL VPN Plug-in that causes an arbitrary code execution.
Strike Mozilla Multiple Products Multiple Header Handling	CWE: 94 CVE: 2011-3000 BID: 49849	When sent an HTTP response with multiple location, content-type, content-length, or content-disposition headers, Mozilla Firefox, Thunderbird, and Seamonkey will use the last header. This increases their susceptibility to newline insertion attacks. This strike will always use multiple location headers as a malicious redirect might, but may additionally use multiple content-type, content-length, and content-disposition headers.
Strike CA ARCserve D2D GWT RPC Information Disclosure	CWE: 200 CVE: 2011-3011 BID: 48897	This strike exploits an information disclosure vulnerability in CA ARCserve. A specially crafted Google Web Toolkit Remote Procedure Call request can be sent to the server, which will return various information, including administrator username and password.
Strike KingView 6.5.3 SCADA ActiveX Control Buffer Overflow	CWE: 119 CVE: 2011-3142 BID: 46757	This strike exploits a vulnerability within KingView 6.5.3. When the ValidateUser method is passed an overly large argument, that data is not properly validated, and a buffer is overflowed allowing for the possibility of remote code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike HP Data Protector dpnepolicyservice Component LogClientInstallation SQL Injection	CWE: 89 CVE: 2011-3156 BID: 50181	This strike exploits a SQL Injection vulnerability in HP Data Protector. A remote, unauthenticated attacker can execute arbitrary SQL commands against the target server.
Strike HP Data Protector dpnepolicyservice Component GetPolicies SQL Injection	CWE: 89 CVE: 2011-3157 BID: 50181	This strike exploits a SQL Injection vulnerability in HP Data Protector. A remote, unauthenticated attacker can execute arbitrary SQL commands against the target server.
Strike HP Data Protector dpnepolicyservice Component RequestCopy SQL Injection	CWE: 89 CVE: 2011-3158 BID: 50181	This strike exploits a SQL Injection vulnerability in HP Data Protector. A remote, unauthenticated attacker can execute arbitrary SQL commands against the target server.
Strike HP Data Protector dpnepolicyservice Component FinishedCopy SQL Injection	CWE: 89 CVE: 2011-3162 BID: 50181	This strike exploits a SQL Injection vulnerability in HP Data Protector. A remote, unauthenticated attacker can execute arbitrary SQL commands against the target server.
Strike Novell Groupwise Messenger Server Process Memory Information Disclosure	CWE: 200 CVE: 2011-3179 BID: 50443	This strike exploits an error in the Novel Groupwise Messenger Server process, which leads to the disclosure of arbitrary content in memory
Strike Microsoft ASP .NET Forms Authentication Elevation of Privilege	CWE: 264 CVE: 2011-3416 BID: 51201	The Forms Authentication feature in the ASP.NET subsystem in Microsoft .NET Framework 1.1 SP1, 2.0 SP2, 3.5 SP1, 3.5.1, and 4.0 allows remote authenticated users to obtain access to arbitrary user accounts via a crafted username, aka "ASP.Net Forms Authentication Bypass Vulnerability."
Strike Oracle Java Rhino Javascript Error Parsing Vulnerability	CVE: 2011-3544 BID: 50218	This strike exploits a remote code execution vulnerability in Oracle Java. The vulnerability can be exploited by overriding the <code>toString</code> method of the <code>Error</code> class within the Rhino JavaScript Engine. Successful exploitation of this vulnerability could result in the execution of arbitrary Java code on the target system.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike TeeChart Professional ActiveX Control Trusted Integer Dereference	CWE: 119 CVE: 2011-4034 BID: 50837	This strike exploits an integer overflow TeeChart ActiveX. The flaw is due to insufficient validation of input to the AddSeries property in the TeeChart ActiveX control. By enticing a user to visit a malicious web page, arbitrary code can be executed on the client system.
Strike HP Network Node Manager OpenView Cross-Site Scripting Vulnerability	BID: 50635 CWE: 79 CVE: 2011-4155	This strike exploits one of five cross-site scripting vulnerabilities in HP OpenView Network Node Manager via HTTP GET request.
Strike HP Network Node Manager Cross-Site Scripting Vulnerability	BID: 50635 CWE: 79 CVE: 2011-4156	This strike exploits one of six cross-site scripting vulnerabilities in HP OpenView Network Node Manager via HTTP POST request.
Strike HP Managed printing Administration jobAcct Remote Command Execution	CWE: 22 CVE: 2011-4166 BID: 51174	This strike exploits a vulnerability in HP Managed Printing Administration web interface. A flaw in the MPAUploader.uploader.1 control, specifically in the UploadFiles function could allow a remote unauthenticated attacker to upload a file under the wwwroot directory. Version 2.6.3 and before are vulnerable.
Strike LibLime Koha Directory traversal and File Upload Vulnerability	CWE: 22 CVE: 2011-4715 BID: 50812	This strike identifies a vulnerability in LibLime Koha that allows for a local file to be uploaded by setting a directory path in the HTTP headers.
Strike HP Easy Printer Care CacheDocumentXMLWithID ActiveX Control Directory Traversal	CWE: 94 CVE: 2011-4786 BID: 51396	HP Easy Printer Care Software contains a directory traversal vulnerability. The flaw is due to a lack of input validation by the CacheDocumentXMLWithId method. An attacker could exploit this vulnerability to create and/or overwrite files, resulting in a denial of service or remote code execution.
Strike Redmine Repository Controller Command Execution	CVE: 2011-4929	This strike exploits a command execution vulnerability in the Redmine repository controller when passing an arbitrary command to the rev parameter.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Nginx NTFS Security Bypass	CWE: 264 CVE: 2011-4963	This strike exploits a security bypass in Nginx when dealing with malformed file name requests.
Strike Microsoft Windows Anti-Cross Site Scripting Library XSS	CWE: 79 CVE: 2012-0007 BID: 51291	This strike exploits a remote cross site scripting flaw in Microsoft Windows Anti-Cross Site Scripting Library.
Strike Microsoft Internet Explorer Information Disclosure	CWE: 200 CVE: 2012-0012 BID: 51932	This strike exploits a vulnerability in Microsoft Internet Explorer where local memory can be disclosed which may contain passwords.
Strike Microsoft Internet Explorer VML Use After Free CVE 2012-0155	CWE: 94 CVE: 2012-0155 BID: 51935	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when removing objects described in the Vector Markup Language (VML).
Strike Microsoft Internet Explorer Select All Use After Free	CWE: 94 CVE: 2012-0171 BID: 52905	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when a select-all operation uses an object after it has been freed.
Strike IBM SPSS SamplePower ActiveX Remote File-System Access	CVE: 2012-0189	This strike exploits a vulnerability in IBM SPSS SamplePower ActiveX control allowing for arbitrary file-system read and write operations.
Strike IBM Tivoli Provisioning Manager Express for Software Distribution Buffer Overflow	CVE: 2012-0198	This strike exploits a vulnerability in IBM Tivoli Provisioning Manager Express for Software Distribution; a buffer overflow in RunAndUploadFile() method allows for arbitrary remote code execution.
Strike IBM Tivoli Provisioning Manager SQL Injection	CWE: 89 CVE: 2012-0199	This strike exploits an SQL Injection in IBM Tivoli Provisioning Manager where an attacker can update underlying data. In particular, a user may upgrade their account to an administrator.

Name	References	Description
Strike Advantech WebAccess HMI and SCADA Software Cross-Site Scripting	CWE: 79 CVE: 2012-0233 BID: 57178	This strike exploits a cross-site scripting vulnerability in Advantech WebAccess. The vulnerability is due to the improper sanitization of user input when creating a new project. An attacker could exploit this vulnerability by creating a project with a malicious description - any user subsequently viewing the project would have have code executed on their machine in the context of the browser.
Strike Broadwin WebAccess Client Bwocxrund ActiveX OcxSpool Format String	CWE: 134 CVE: 2012-0242 BID: 57178	This strike exploits a format string vulnerability in Broadwin WebAccess ActiveX control. The vulnerability is due to the improper sanitization of the OcxSpool method. By enticing a user to view a malicious web page, an attacker could execute arbitrary code on the victim machine in the context of the user.
Strike NTR ActiveX Control StopModule() Remote code execution	CWE: 20 CVE: 2012-0267 BID: 51374	This strike exploits a vulnerability in the NTR ActiveX suite. Specifically, due to improper handling of parameters in the StopModule() method, a memory corruption can be triggered that leads to code execution. All versions before 2.0.4.8 are vulnerable.
Strike Linksys PlayerPT ActiveX control sUrl Parameter Buffer Overflow	BID: 54588 CWE: 119 CVE: 2012-0284	This strike identifies a buffer overflow vulnerability in Linksys' ActiveX control, PlayerPT. Improper validation occurs when handling the sUrl parameter, and an overly large user supplied value will overflow the buffer that is allocated on the stack for the parameter.
Strike Symantec Web Gateway timer.php XSS	CWE: 79 CVE: 2012-0296 BID: 53396	This strike exploits a cross site scripting vulnerability in Symantec Web Gateway Management Console.
Strike apache struts2 cookie OGNL command execution	CWE: 264 CVE: 2012-0392	This strike exploits a command execution vulnerability in Apache struts2. This vulnerability is due to no input check the cookie names. Remote attackers may do arbitrary code execution on the target system.
Strike Oracle AutoVue ActiveX control Buffer Overflow	BID: 53077 CVE: 2012-0549	This strike exploits a vulnerability in Oracle AutoVue Enterprise Visualization software. When a string is passed to the SetMarkupMode method with a size greater than 0x100, that string is copied from heap memory into an allocated stack buffer without validation.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle GlassFish XSS	BID: 53136  CVE: 2012-0551	This strike exploits a cross site scripting flaw in the Oracle GlassFish. The remote attacker could use this vulnerability to do code execution attack in the target system.
Strike Apple Quicktime Plugin SetLanguage Buffer Overflow	CWE: 119  CVE: 2012-0666  BID: 53577	Apple QuickTime Plugin contains a buffer overflow vulnerability. The length of the SetLanguage parameter is not verified, and thus can be exploited to execute arbitrary code or crash the plugin/browser.
Strike IBM Rational ClearQuest CQOLE ActiveX Remote Code Execution	BID: 53170  CWE: 119  CVE: 2012-0708	This strike that exploits IBM's Rational ClearQuest CQOLE ActiveX controls RegisterSchemaRepoFromFileByDbSet() method; a function prototype mismatch allows remote attacker to control the returned function pointer.
Strike Tiki Wiki PHP Unserialize Code Execution	CWE: 94  CVE: 2012-0911  BID: 54298  EXPLOITDB : 19573  EXPLOITDB : 19630	This strike exploits a code execution vulnerability in Tiki Wiki. Certain configurations of Tiki Wiki will allow writing of arbitrary PHP code via the printpages parameter of the tiki-print_multi_pages script. A specially crafted HTTP request can write and call arbitrary PHP code, resulting in arbitrary code execution.
Strike LANDesk ThinkManagement Suite ServerSetup.asmx Directory Traversal	CWE: 264  CVE: 2012-1195  BID: 52023	This strike exploits a directory traversal vulnerability in the LANDesk ThinkManagement Suite allowing arbitrary file creation and command execution.
Strike LANDesk ThinkManagement Arbitrary File Deletion	BID: 52023  CWE: 22  CVE: 2012-1196	This strike exploits a weakness in the LANDesk ThinkManagement Suite where an arbitrary file may be deleted.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike D-link DSL-2640B Router Admin password change	BID: 52096 CWE: 352 CVE: 2012-1308	This strike exploits a vulnerability in D-Link DSL-2640B Router's web interface which listens on port 80. You are able to change router parameters as well as the administrator's password
Strike WebCalendar settings.php Code Injection and Remote Code Execution	CVE: 2012-1495	This strike identifies a vulnerability inside WebCalendar version 1.2.4 and prior. There exists a code injection and modification vulnerability by which modifications made to the settings.php script are possible because they are not properly validated. Updating this script will allow the attacker to execute code remotely.
Strike Microsoft Internet Explorer Layout Object Use After Free	CWE: 119 CVE: 2012-1526 BID: 54950	This strike exploits a vulnerability within Microsoft Internet Explorer. The vulnerability exists within the layout engine, and when an invalid object is contained by elements that have a large negative margin value , a CTreeNode object can be destroyed. This results in a use-after-free error when trying to access that object later and possibly memory corruption.
Strike Oracle WebCenter Forms Recognition ActiveX Code Execution	CVE: 2012-1709	This strike exploits a vulnerability in the Oracle WebCenter Forms Recognition ActiveX control. A lack of path validation in Save() method allows the remote attacker to potentially execute arbitrary code.
Strike Oracle WebCenter Forms Recognition ActiveX Control Code Execution	CVE: 2012-1710	This strike exploits a vulnerability in the Oracle WebCenter Forms Recognition ActiveX control. A lack of path validation in SaveLayout() method allows the remote attacker to potentially execute arbitrary code.
Strike PHP CGI Command Execution	CWE: 20 CVE: 2012-1823	This strike exploits a vulnerability in PHP framework, more specifically how CGI scripts is handled. By improper input escaping, malicious php.ini directives can be supplied to the php executable and any arbitrary script can be interpreted and executed on the server. All versions of PHP prior to 5.3.12 and 5.4.2 are vulnerable.
Strike Microsoft SharePoint Reflected List inplnview Parameter Cross Site Scripting Vulnerability	CWE: 79 CVE: 2012-1863 BID: 54316	Microsoft Office Sharepoint contains a cross-site scripting (XSS) vulnerability. The vulnerability is due to insufficient validation of the list parameters passed to the inplnview.aspx page.
Strike Microsoft Internet Explorer Table Element Row Insertion Memory Corruption	CWE: 94 CVE: 2012-1880	This strike exploits a vulnerability that exists in Microsoft Internet Explorer. If the methods getClientRects(), or getBoundingClientRect() are used to call Table elements, and then a row is inserted into those element that contain a caption, memory corruption occurs.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft ActiveX Objects Cachesize Memory Corruption	CWE: 119 CVE: 2012-1891	This strike demonstrates the vulnerability within Microsoft ActiveX Data Objects. When creating a recordset from an XML data island, a heap buffer is allocated based on the CacheSize property. This code is not properly validated, and if the value is large enough a NULL pointer is returned as a pointer for a different array.
Strike Mozilla Firefox Thunderbird and Seamonkey Table Memory Corruption	BID: 54578 CWE: 399 CVE: 2012-1952	This Strike exploits a vulnerability in the Mozilla products, Firefox, Thunderbird, and Seamonkey. An object casting mismatch occurs when handling a mixed assortment of columns and rows within a table. If a col based frame is received first followed by a row element, the object type is not verified, and the code is mistakenly viewed as a column group.
Strike IMB Lotus Notes URL handling command execution	CWE: 94 CVE: 2012-2174 BID: 54070	IBM Lotus notes has a command execution vulnerability. If a notes: URI containing the strings "-RPARAMS" followed by "-vm" is accessed, arbitrary remote code could be executed.
Strike IBM Lotus iNotes ActiveX Control Attach_Times Buffer Overflow	CWE: 119 CVE: 2012-2175	This strike exploits a vulnerability in IBM Lotus iNotes ActiveX control. If the General_Mode property is equal to 1 the Attachment_Times property is parsed as date time strings. This is stored in a 0x200 byte stack buffer, and if the string too large it will write into it.
Strike IBM Lotus Quickr QuickPlace ActiveX Control Remote Code Execution	BID: 53678 CWE: 119 CVE: 2012-2176	This strike exploits a vulnerability in the IBM Lotus Quickr QuickPlace ActiveX control. Lack of boundary checking causes a string copy in either Attachment_Times or Import_Times properties to write past the end of a buffer.
Strike GE Proficy Historian ActiveX Remote Code Execution	CWE: 78 CVE: 2012-2516	This strike exploits a vulnerability within GE Proficy Historian's ActiveX control KeyHelp.ocx. Specifically while using the LaunchTriPane method to run a chm file using hh.exe, the method fails to validate the parameters when passed the decompile option. This parameter can be passed a remote UNC path as the location of the stored chm file to be decompiled to a specified directory on the local machine. This strike demonstrates what would happen by calling a locally stored chm file on a windows machine to be decompiled to the C:/ directory. The path of the locally stored (safe) chm in this demonstration would be replaced by the remote UNC path and malicious chm file
Strike Microsoft Internet Explorer CSS Mailto Use After Free Condition	CWE: 94 CVE: 2012-2521	This strike exploits a vulnerability a Use After Free condition in Microsoft Internet Explorer. If a mailto URL is passed as a src parameter in the CSS font-face rule of the CSS style, a dialog box will be launched by a DOM object trying to access the font. If this object is then later destroyed, a UAF condition occurs when an event handler tries to access it.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer JScript and VBScript Integer Overflow	CWE: 189 CVE: 2012-2523	This strike exploits a vulnerability in the Microsoft JavaScript and VBscript engines. An integer overflow exists when handling strings. The code extends the 32bit value to a 64bit value and this is used as the size parameter when calling memcpy. If a string greater than 0x80000000 is passed in as this parameter an integer overflow occurs which leads to memory corruption.
Strike Microsoft System Center Configuration Manager Cross Site Scripting	BID: 55430 CWE: 79 CVE: 2012-2536	This strike exploits a reflected cross-site scripting (XSS) vulnerability in Microsoft System Center Configuration Manager. The vulnerability is caused by lack of input validation when handling HTTP requests. This vulnerability can be exploited by an attacker to execute malicious code in the context of the victim user's browser.
Strike Symantec Web Gateway blocked.php Blind SQL Injection	CWE: 89 CVE: 2012-2574 BID: 54424	This Strike exploits Symantec Web Gateway with a blind SQL injection in blocked.php. The strike will attempt to create a new user in the database.
Strike Ruby on Rails Where Hash SQL Injection	BID: 53970 CWE: 89 CVE: 2012-2695	This strike exploits a SQL injection vulnerability Ruby on Rails. The vulnerability results from a lack of input validation while handling hash values. A remote attacker could exploit this vulnerability by sending malicious SQL code.
Strike Symantec Web Gateway pbcontrol.php RCE	CWE: 78 CVE: 2012-2953 BID: 54426	This strike exploits pbcontrol.php in Symantec Web Gateways, which fails to correctly check the filename parameter before using it in an exec call. No authentication is needed.
Strike Symantec Web Gateway languageTest.php Root RCE	CWE: 264 CVE: 2012-2957 BID: 54429	This strike exploits web-server logs and a bug in languageTest.php in Symantec Web Gateway to execute code as root.
Strike Webmin show.cgi URI Path Command Execution	CVE: 2012-2982 BID: 55446	This strike exploits a vulnerability in Webmin. If the URI portion of the show.cgi command contains a correctly placed pipe character " ," the URI will run as a shell command at root level. Successful exploitation will allow for command execution at root level.

Name	References	Description
Strike Trend Micro Control Manager ad hoc query Module SQL Injection	CWE: 89 CVE: 2012-2998	This strike exploits an SQL injection vulnerability in Trend Micro Control Manager. The vulnerability is due to a insufficient sanitization of input when handling parameters to the AdHocQuery_Processor.aspx page. Specifically the id parameter is used, unsanitized, to build an SQL query. If the parameter value contains a single quote ('), the literal id value will be terminated and any SQL code following will be added to the constructed SQL query that is executed by the Control Manager server. An attacker can exploit this vulnerability by sending a specially crafted request to the AdHocQuery_Processor.aspx page with an id parameter injecting SQL code. Successful exploitation could result in arbitrary execution of SQL queries with DB Administrator privileges.
Strike Oracle Reports Developer URLPARAMETER remote execution	BID: 55955 CVE: 2012-3152	This strike exploits a vulnerability in the Oracle Reports Developer Software suite. Specifically the vulnerability allows posting random javascript inside the executable path of the server and eventually achieve code execution. All versions of Oracle Fusion Middleware 11.1.1.4, 11.1.1.6, and 11.1.2.0 are vulnerable to this attack.
Strike Oracle Reports Developer PARSEQUERY information disclosure	CVE: 2012-3153 BID: 55961	This strike exploits a vulnerability in the Oracle Reports Developer Software suite. Specifically, when using the PARSEQUERY functionality inside the rw servlet , a malicious user could potentially manipulate the system into divulging database usernames and passwords. All versions of Oracle Fusion MiddleWare 11.1.1.4, 11.1.1.6 and 11.1.2.0 are vulnerable to this attack.
Strike HP SiteScope SOAP Call Remote Arbitray File Access	CVE: 2012-3259 CVE: 2012-3260 BID: 55269	This strike exploits one of two security bypass vulnerabilities in HP SiteScope. The vulnerability is due to lack of proper access control by the APIMonitorImpl web service, using the getFileInternal and loadFileContent functions. Remote, unauthenticated users can exploit these vulnerabilities to read arbitrary system files.
Strike HP SiteScope SOAP Call APIPreferenceImpl Multiple Security Bypass	CVE: 2012-3261 BID: 55269	This strike exploits a security bypass vulnerability in HP SiteScope. The vulnerability is due to lack of authentication checking by the SOAP Call API. Remote, unauthenticated users can create new users as well view plaintext credential information simply by sending a well-formed SOAP request.
Strike HP SiteScope Multiple Directory Traversal Vulnerabilities	CVE: 2012-3264 BID: 55273	This strike exploits a directory traversal vulnerability in HP SiteScope. The vulnerability is due to insufficient validation of user-supplied input by Upload/Download manager servlets while processing http requests. A remote attacker could exploit the vulnerability to download, or upload and execute, arbitrary files to/from the target server via relative or full directory paths.
Strike Zend Technologies Zend Framework Zend_XmlRpc SimpleXMLElement Information Disclosure	CVE: 2012-3363 BID: 54192	This strike exploits an information disclosure vulnerability in Zend Technologies Zend Framework. A user can POST a crafted XML file and receive content of arbitrary files.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Apache x-forwarded-for Denial of Service in mod_rpaf	BID: 55154  CVE: 2012-3526	This strike exploits a denial of service flaw in Apache's mod_rpaf module when presented with an invalid x-forward-for tag. Note that Apache's thread model and restart capabilities may somewhat mask the observable behavior of this exploit.
Strike Apple Safari 5.1.7 And Prior Title Memory Corruption	BID: 55534  CVE: 2012-3684	This strike exploits a memory corruption vulnerability in Safari 5.1.7 and before (both desktop and mobile).
Strike Apple Quicktime Plugin Content-Type Header Buffer Overflow	CWE: 119  CVE: 2012-3753  BID: 56438	Apple QuickTime Plugin contains a buffer overflow vulnerability. The length of the Content-Type parameter is not verified, and thus can be exploited to execute arbitrary code or crash the plugin/browser.
Strike Apple Quicktime Player ActiveX Control Code Execution Vulnerability	CWE: 399  CVE: 2012-3754  BID: 56438	This strike exploits a vulnerability in Apple Quicktime Player's QTplugin. Specifically a use-after-free error condition occurs when the clear method is called. The code frees an internal object that can be referenced by Internet Explorer later.
Strike Samsung Kies Arbitrary Command Execution	CVE: 2012-3807	This strike exploits an input validation error in Samsung Kies ActiveX controls that allows for an arbitrary command execution.
Strike Avayas IP Office Customer Call Reporter Unrestricted File Upload	CVE: 2012-3811  BID: 54225	This strike exploits a flaw in Avaya's IP Office Customer Call Reporter where an unauthenticated user can upload an arbitrary file.
Strike Mozilla Firefox WAV Processing Heap Overflow	CWE: 119  CVE: 2012-4186  BID: 56135	This strike exploits a Memory Corruption vulnerability in Mozilla Firefox. The vulnerability is due to error while processing wav files. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, possibly leading to execution of arbitrary code on the victim machine.
Strike Mozilla Firefox Cross Domain Information Disclosure	CWE: 264  CVE: 2012-4192	This strike exploits a vulnerability in Mozilla Firefox. This vulnerability violates the same origin policy which prevents a document or script loaded from one origin from getting or setting properties of a document from another origin. This document can read the property of the window object with a different origin, which leads to the disclosure of the URL information for that window object.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike WordPress Plugin Quick Post Widget 1.9.1 Cross-site scripting	CWE: 79 CVE: 2012-4226 BID: 54311	WordPress Quick Post Widget plugin contains multiple cross-site scripting vulnerabilities.
Strike Symantec Messaging Gateway Information Disclosure	CWE: 22 CVE: 2012-4347 BID: 56789	This strike exploits one of two directory traversal vulnerabilities exist in Symantec Messaging Gateway. The vulnerabilities are cause by improper validation of user-supplied input, specifically HTTP parameters. A remote attacker could exploit these vulnerabilities to download arbitrary system files.
Strike Java Sandbox Breach	BID: 55213 CVE: 2012-4681	This strike demonstrates an exploit in Java where an attacker can run arbitrary Java code without sandbox protection.
Strike Microsoft Internet Explorer HTML Style Property Reference Counting Use After Free	CWE: 399 CVE: 2012-4787 BID: 56830	Microsoft Internet Explorer contains a use after free vulnerability. When handling HTML styles, if the style property of an object is not supported by Internet Explorer, the object is not properly added to the Document Object Model. After the object is deleted, a use after free condition occurs due to improper reference counting. Successful exploitation may result in execution of arbitrary code or abnormal termination of Internet Explorer.
Strike Asus Net4Switch ActiveX control Buffer Overflow	CWE: 119 CVE: 2012-4924 BID: 52110	This strike exploits a vulnerability within Asus' Net4Switch ActiveX control ipswcom.dll. This vulnerability exists within the alert and msgbox methods. When a string is passed to either of these it is not properly validated, and if it is larger than 0x7D0 bytes it will overflow the buffer when copied into it.
Strike Novell ZENWorks Asset Management Backdoor User and Password	CWE: 255 CVE: 2012-4933	This strike exploits a backdoor username and password in Novell's ZENWorks Asset Management. This account is hardcoded into the source and cannot be disabled.
Strike Novell File Reporter FSFUI Arbitrary File Retrieval	CWE: 22 CVE: 2012-4958	This strike exploits a file retrieval vulnerability in Novell File Reporter. The vulnerability is caused by insufficient authentication when handling FSFUI requests. An remote unauthenticated attacker could exploit this vulnerability by sending a specially crafted request to the server. Successful exploitation could result in arbitrary file retrieval with SYSTEM privileges.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Java Sandbox Breach via Glassfish	CVE: 2012-5076  BID: 56054	This strike demonstrates an exploit in Java where an attacker can run arbitrary Java code without sandbox protection by leveraging an exploit in the glassfish package.
Strike phpmyadmin 3.5.2.2 Backdoor Access and Code Execution	CWE: 94  CVE: 2012-5159  BID: 55672	This Strike exploits a vulnerability in phpmyadmin that allows for code to be executed through a backdoor.
Strike HP Intelligent Management Center Arbitrary File Upload	CVE: 2012-5201  BID: 58385	This strike exploits a flaw in HP's Intelligent Management Center where a user can upload a zip file which in turn clobbers arbitrary files.
Strike HP Intelligent Management Center File Disclosure	CVE: 2012-5202  BID: 58385	This strike exploits a vulnerability in HP's Intelligent Management Center where an unauthenticated user may download an arbitrary file.
Strike HP Intelligent Management Center File Disclosure Traversal	CVE: 2012-5203  BID: 58385	This strike exploits a vulnerability in HP's Intelligent Management Center where a user can download an arbitrary file.
Strike HP Intelligent Management Center ict File Disclosure Traversal	CVE: 2012-5204  BID: 58385	This strike exploits a vulnerability in HP's Intelligent Management Center where an unauthenticated user may download an arbitrary file.
Strike HP Intelligent Management Center syslog File Disclosure	CVE: 2012-5206  BID: 58385	This strike exploits a vulnerability in HP's Intelligent Management Center where an unauthenticated user may download an arbitrary file.
Strike HP Intelligent Management Center download File Disclosure	CVE: 2012-5208  BID: 58385	This strike exploits a vulnerability in HP's Intelligent Management Center where an unauthenticated user may download an arbitrary file.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike HP Intelligent Management Center imc File Disclosure	CVE: 2012-5211 BID: 58385	This strike exploits a vulnerability in HP's Intelligent Management Center where an unauthenticated user may download an arbitrary file.
Strike Adobe Flash Player Memory Corruption	CWE: 119 CVE: 2012-5271	This strike exploits a flaw in Adobe's Flash Player where a malformed action script can write variables which are not allocated and leads to memory corruption.
Strike TVMOBili HTTP Request Denial of Service	BID: 56853 CWE: 119 CVE: 2012-5451	This strike exploits a denial of service in TVMOBili when sending an specifically crafted HTTP request to the service listneing on port 30888.
Strike lighttpd Connection Type Denial of Service	CWE: 399 CVE: 2012-5533 BID: 56619	This strike exploits a denial of service bug in lighttpd where a remote user can pass in a malformed connection type which forces the server into an infinite loop.
Strike Squid Proxy Cache Resource Exhaustion	CWE: 20 CVE: 2012-5643	This strike exploits a resource exhaustion vulnerability in Squid Proxy Cache Manager. Memory is allocated on the server to store parameters based only on the Content-Length header, when handling http requests. If an overly large Content-Length value is used then large amounts of data in the body can be used to fill an allocated buffer causing RAM to fill up and possibly a denial of service condition to occur.
Strike VMware vSphere API SOAP Request Denial Of Service	BID: 56571 CWE: 20 CVE: 2012-5703	This strike exploits a mishandling of a tag in the vSphere API which causes the hostd service to terminate for ESX/ESXi servers, causing a denial of service.
Strike McAfee Virtual Technician ActiveX Save File Creation-File Overwrite	CWE: 264 CVE: 2012-5879 BID: 58750	This strike exploits a vulnerable ActiveX control in McAfee Virtual Technician. The Save method allows for creation or overwriting of arbitrary files, including important system files. Successful exploitation could result in creation or overwriting of arbitrary files with privileges of the currently logged in user. Overwriting of system files could result in a denial of service condition.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Quest InTrust Annotation Objects ActiveX Control Index out of Bounds	CVE: 2012-5896 BID: 52765	This strike exploits a memory access vulnerability in Quest InTrust. The vulnerability is due to a flawed ActiveX control, which allows a user to specify a function pointer. A remote, unauthenticated attacker could exploit this vulnerability by enticing a user to view a specially crafted web page.
Strike IBM SPSS SamplePower ActiveX Buffer Overflow	CWE: 119 CVE: 2012-5946 BID: 59559	This strike exploits an IBM SPSS SamplePower ActiveX control buffer overflow vulnerability. Remote attackers can use this vulnerability to let target user to execute arbitrary code.
Strike IBM SPSS SamplePower VSFlexGrid ActiveX Buffer Overflow	CWE: 119 CVE: 2012-5947 BID: 59556	This strike exploits a vulnerable ActiveX control in IBM SPSS SamplePower. The ComboList and ColComboList values in the VSFlexGrid ActiveX control will copy a string to a buffer without validation. Successful exploitation can result in arbitrary code execution or abnormal termination of the browser.
Strike Digium Asterisk Server Stack Buffer Overflow	CWE: 119 CVE: 2012-5976	This strike exploits a defect in Digium's Asterisk Server where a malformed user request to a web page can clobber a stack buffer.
Strike Nagios history.cgi host buffer overflow	CWE: 119 CVE: 2012-6096 BID: 56879	This strike exploits a stack buffer overflow vulnerability in Nagios. History.cgi fails to validate the length of the host parameter. A sufficiently long host parameter can be used to overflow a stack buffer. Successful exploitation could result in execution of arbitrary code with privileges of the Nagios program or abnormal program termination, resulting in a denial of service condition.
Strike Microsoft Internet Explorer removeChild Use After Free	CWE: 399 CVE: 2013-0021	This strike exploits a vulnerability in Microsoft's Internet Explorer where Javascript can modify a document and attempt to reuse data after it has been freed.
Strike Microsoft Internet Explorer SLayoutRun Use After Free Vulnerability	CWE: 399 CVE: 2013-0025 BID: 57830	This strike exploits a remote code execution vulnerability in Microsoft Internet Explorer (IE). The vulnerability occurs when Internet Explorer attempts to access a previously freed object. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer CPasteCommand Use After Free Vulnerability	CWE: 399 CVE: 2013-0027 BID: 57831	This strike exploits a remote code execution vulnerability in Microsoft Internet Explorer (IE). The vulnerability occurs when Internet Explorer attempts to access a previously freed object. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.
Strike Microsoft Internet Explorer On Before Edit Event Use After Free	CWE: 399 CVE: 2013-0029	This strike exploits a vulnerability in Microsoft's Internet Explorer where Javascript can modify a document and attempt to reuse data after it has been freed.
Strike Microsoft Internet Explorer VML Memory Corruption	CWE: 119 CVE: 2013-0030	A code execution vulnerability has been reported in Microsoft Internet Explorer. The vulnerability is due to memory corruption when parsing Vector Markup Language. A remote attacker could exploit this vulnerability by enticing the target user to open a malicious web page. On successful exploitation, arbitrary code would be executed in the security context of the currently logged-in user.
Strike Microsoft SharePoint CallbackFn Cross Site Scripting	CWE: 264 CVE: 2013-0080 BID: 58371	Microsoft SharePoint contains a cross site scripting vulnerability. The functions CallbackFn and CallbackParams do not sanitize for JavaScript. If a user clicks a link with JavaScript contained in these parameters, the JavaScript will execute with browser privileges. Successful exploitation can result in information disclosure or execution of JavaScript commands.
Strike Microsoft Internet Explorer onResize Use After Free Vulnerability	CWE: 399 CVE: 2013-0087 BID: 58341	This strike exploits a remote code execution vulnerability in Microsoft Internet Explorer (IE). The vulnerability occurs when Internet Explorer attempts to access a previously freed object. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.
Strike Microsoft Internet Explorer saveHistory Use After Free Vulnerability	CWE: 399 CVE: 2013-0088 BID: 58342	This strike exploits a remote code execution vulnerability in Microsoft Internet Explorer (IE). The vulnerability occurs when Internet Explorer attempts to access a previously freed object. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.
Strike Microsoft Internet Explorer CMarkupBehaviorContext Use After Free Vulnerability	CWE: 399 CVE: 2013-0089 BID: 58343	This strike exploits a remote code execution vulnerability in Microsoft Internet Explorer (IE). The vulnerability occurs when Internet Explorer attempts to access a previously freed object. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Honeywell Multiple Products HSCRemoteDeploy RemoteInstaller ActiveX Code Execution	CWE: 94 CVE: 2013-0108 BID: 58134	This strike exploits a code execution vulnerability in multiple Honeywell products. The HSCRemoteDeploy.RemoteInstaller ActiveX control found in the Honeywell HMIWeb Browser can be used to access and execute an arbitrary HTML application. Successful exploitation could allow for execution of arbitrary code with user privileges.
Strike Ruby on Rails Action Pack Type Casting Parameter Parsing Vulnerability	CWE: 20 CVE: 2013-0156 BID: 57187	This strike exploits a remote code execution vulnerability in Ruby on Rails. The vulnerability is due to a type casting in the Ruby on Rails XML processor. Exploiting this vulnerability could allow remote attackers to execute arbitrary code on the target server.
Strike Movable Type 4.2x, 4.3x Upgrade Script RCE	CWE: 287 CVE: 2013-0209 CVE: 2012-6315	This strike exploits Movable Type 4.2x, 4.3x upgrade script to gain remote code execution on target server.
Strike MiniUPnPd SOAP Remote Code Execution	CWE: 119 CVE: 2013-0230 BID: 57608	This strike identifies a vulnerability in MiniUPnP server. A SOAP action sent to the server with a crafted HTTP header can overflow a stack buffer allowing for remote code to be executed.
Strike Ruby on Rails JSON Processor YAML Deserialization Vulnerability	CVE: 2013-0333 BID: 57575	This strike exploits a remote code execution vulnerability in Ruby on Rails. The vulnerability is due to an input validation error when deserializing YAML using JSON processor. Exploiting this vulnerability could allow remote, unauthenticated attackers to execute arbitrary code on the target server.
Strike Oracle Application Framework Diagnostic and Developer Mode Information Disclosure	CVE: 2013-0397	This Strike identifies a vulnerability in Oracle Application Framework, in which a user can access diagnostic and developer modes without having to be authenticated. By setting either of these parameters a user can perform a number of tracing and logging functions that provide the user with sensitive information like settings, session information and passwords.
Strike Adobe ColdFusion scheduleedit.cfm Authentication Bypass	CWE: 255 CVE: 2013-0625 BID: 57164	This strike exploits an authentication bypass vulnerability in Adobe ColdFusion. The flaw is due to a lack of authentication validation by the ColdFusion administration web console when creating a scheduled task. A remote unauthenticated attacker could exploit this vulnerability by enticing an authenticated user to view a malicious web page. Exploitation of this vulnerability could allow an attacker to upload malicious code to be executed at a scheduled time.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Adobe ColdFusion rdsPasswordAllowed Authentication Bypass Vulnerability	CWE: 276 CVE: 2013-0632	This strike exploits a authentication bypass vulnerability in the web component of Adobe ColdFusion. The vulnerability is due to incorrect default permissions. A remote unauthenticated attacker could exploit this vulnerability by send a specially crafted request. Successful exploitation could allow an attacker to bypass authentication mechanisms and gain unauthorized admin access to the application.
Strike Siemens SIMATIC RegReader ActiveX Buffer Overflow	CWE: 119 CVE: 2013-0674	This strike exploits a vulnerability in Siemen's SIMATIC RegReader where a malformed parameter inside an ActiveX control can clobber a buffer.
Strike Novell GroupWise ActiveX Pointer Dereference	CWE: 78 CVE: 2013-0804	This strike exploits a vulnerability in Novell's GroupWise Client where a malformed ActiveX control can dereference an arbitrary pointer which can lead to a crash.
Strike Oracle Java 2D ImagingLib Integer Overflow	CVE: 2013-0809 BID: 58296	This strike exploits a remote code execution vulnerability in Oracle Java. The vulnerability is due to an integer overflow in the ImagingLib class, in the use of BufferedImage method. Successful exploitation of these vulnerabilities could result in the execution of arbitrary Java code on the target system.
Strike Novell ZENworks Configuration Management umaninv Information Disclosure	CWE: 22 CVE: 2013-1084	This strike exploits a information disclosure vulnerability that can be triggered by sending malicious HTTP requests. The request can be crafted to traverse directories and as such access any file on disk.
Strike Novell Messenger Client Stack Buffer Overflow	CWE: 119 CVE: 2013-1085	This strike exploits a vulnerability in Novell's Messenger Client where a malformed href response refers to a file that doesn't exist and the resulting error message can clobber a stack buffer.
Strike Microsoft HTTP Denial of Service	CWE: 399 CVE: 2013-1305	This strike exploits a denial of service in Microsoft's handling of malformed HTTP requestes.
Strike Internet Explorer .ipsum Construct Layout Memory Corruption	CWE: 416 CVE: 2013-1310 BID: 59751	This strike exploits a Memory Corruption vulnerability in Inernet Explorer. The vulnerability is due to error while handling CSS psuedo-objects. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike SonicWall Multiple Products setSessionCheck Authentication Bypass	CVE: 2013-1359 BID: 57445	This strike exploits a vulnerability that is present in multiple SonicWall products and that allows remote unauthenticated access. The vulnerability is located at the level of the applianceMainPage
Strike DataLife Engine 9.7 Remote Code Execution	CWE: 94 CVE: 2013-1412 BID: 57603	Due to improper sanitization of user-supplied input into a preg_replace function in DataLife Engine 9.7, it is possible to gain remote code execution on the target system
Strike Piwigo Photo Gallery Project LocalFiles Editor Plugin Cross Site Request Forgery	CWE: 352 CVE: 2013-1468	This strike exploits a vulnerability in the LocalFiles Editor in Piwigo versions 2.4.6 and prior. A cross site request forgery attack exists that allows for the attacker to trick an administrator into visiting a malicious page which can create and execute PHP files.
Strike Piwigo Photo Gallery Project install script Directory Traversal	CWE: 22 CVE: 2013-1469 BID: 58229	This strike exploits a vulnerability in the Piwigo install.php script. Specifically a user is able to navigate outside of the restricted path and gain access to and delete arbitrary files.
Strike Oracle Document Capture BlackIceDevMode SetAnnotationFont ActiveX Buffer Overflow	CVE: 2013-1516 BID: 59112	This strike exploits a vulnerable ActiveX control in Oracle Document Capture. An overly long IfFaceName parameter in the SetAnnotationFont function of the BlackIceDevMode ActiveX control will overflow a stack buffer. Successful exploitation may result in arbitrary code execution or abnormal termination of the client web browser.
Strike Dlink IP Camera Authenticated Arbitrary Command Execution	CVE: 2013-1599	This strike exploits a command execution vulnerability inside Dlink's IP Cameras through a improperly parsed parameter supplied to a cgi script.
Strike Mozilla Firefox crypto.generateCRMFRequest Peek into Privileged Callers Scope	CWE: 20 CVE: 2013-1710 BID: 61900	This strike exploits a vulnerability in Mozilla Firefox. It is possible to craft Javascript in such a way that allows remote attackers to execute arbitrary JavaScript code or conduct cross-site scripting attack when calling the crypto.generateCRMFRequest function. This can lead to remote code execution on the victim's machine.
Strike Apache Rave v.11-.20 User Information Disclosure	CWE: 200 CVE: 2013-1814	This Strike exploits a information disclosure vulnerability in Apache Rave .11-.20. An authenticated user can retrieve the complete users object information by querying the correct path.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Squid Proxy Server Accept Language Denial of Service	BID: 58316 CWE: 20 CVE: 2013-1839	This strike exploits a flaw in the Squid Proxy Server where a malformed language name will put the server into an infinite loop.
Strike Apache HTTP Server RewriteLog Command Execution	CWE: 310 CVE: 2013-1862 BID: 59826	This strike identifies a vulnerability in the Apache HTTP Server mod_Rewrite module. This module has a logging feature that can be triggered that will record URL requests to a log file. Due to improper sanitation of these requests an attacker can send a URI that encodes a command to be executed when the mod_rewrite module logs the request. If the target views and then presses enter the command will be executed with the privileges of the current logged in user.
Strike Apache HTTP Server Merge Denial of Service	BID: 61129 CWE: 264 CVE: 2013-1896	This strike exploits a denial of service vulnerability in Apache HTTP server. The vulnerability is due to lack of input sanitation in the http request.
Strike Wordpress W3 Total Cache PHP Code execution	BID: 59316 CVE: 2013-2010	This strike exploits a vulnerability in the two popular Wordpress plugins, w3-total-cache and wp-super-cache. Both plugins can handle dynamic content on the page. Multiple tags specific to the plugins are interpreted as HTML comments by wordpress and but, they are interpreted and executed on the server. A malicious attacker can exploit this by inserting scripts inside HTML comments and thus successfully leverage server side code execution. All versions of W3 Supercache prior to 1.2 as well as W3 Total Cache prior to 0.9.2 are vulnerable.
Strike PHP php_quot_print_encode parameter parsing heap buffer overflow	CWE: 119 CVE: 2013-2110 BID: 60411	This strike exploits a buffer overflow vulnerability in PHP. When parsing percent encoded parameters, specially crafted strings can cause a heap buffer overflow. Successful exploitation may allow arbitrary code execution or abnormal termination of application using php, resulting in a denial of service condition.
Strike Apache Struts URL Command Execution	CWE: 94 CVE: 2013-2115 BID: 60167	This strike exploits command execution vulnerability in Apache Struts. A specially crafted URL can be sent to enable allowStaticMethodAccess and execute arbitrary Java runtime commands. Successful exploitation can result in execution of arbitrary code.

Name	References	Description
Strike Apache Struts2 wildcard OGNL command execution	BID: 60346 BID: 64758 CWE: 94 CVE: 2013-2134	This strike exploits a command execution vulnerability in Apache struts2. This vulnerability is due to no input check the ognl action name in http request. Remote attackers may do arbitrary code execution on the target system.
Strike Apache Struts OGNL action- redirect- redirectAction Command Execution	CWE: 20 CVE: 2013-2251 BID: 61189	This strike exploits command execution vulnerability in Apache Struts. A specially crafted HTTP GET or POST requests can be sent to the Apache Struts server to execute arbitrary code with user privileges.
Strike HP System Management Homepage iprange Stack Buffer Overflow	CWE: 121 CVE: 2013-2362	A stack buffer overflow exists in HP System Management Homepage. The vulnerability is due to insufficient input validation when handling HTTP requests containing an iprange variable to the /proxy/DataValidation URI. A remote unauthenticated attacker could exploit this vulnerability by sending a crafted request to the vulnerable service. Successful exploitation could result in arbitrary code execution in the context of the currently affected service, which is System by default.
Strike HP SiteScope SOAP call code execution	CVE: 2013-2367	This strike exploits a code execution vulnerability in HP SiteScope SOAP. This vulnerability is due to lack of checking the ahs key value which may be followed by malicious command. Attack can use this vulnerability to do command injection attack on the target system.
Strike HP LoadRunner micWebAjax.dll ActiveX Control Vulnerability	CVE: 2013-2368 BID: 61436	This strike exploits a vulnerability within HP LoadRunner. The vulnerability is due to insufficient boundary checking of micWebAjax parameters. By enticing a user to view a malicious web page an attacker could execute arbitrary code in the security context of the user.
Strike HP LoadRunner lrFileIOService WriteFileBinary ActiveX Control Pointer Input Validation Error	CVE: 2013-2370 BID: 61441	This strike exploits a vulnerable ActiveX control in HP LoadRunner. The WriteFileBinary method in the lrFileIOService ActiveX Component takes a parameter used as a pointer, which can be used to point to invalid memory, causing abnormal termination, or a valid address to alter program flow.
Strike Oracle Java Final Field Overwrite Remote Code Execution	CWE: 265 CVE: 2013-2423	This strike exploits a design weakness vulnerability in Oracle Java JRE/JDK. This vulnerability is due to improper validation of user supplied input. A remote attacker could exploit this vulnerability by enticing a user to open a crafted webpage and can result in remote code execution in the context of the user running the browser.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle Java java.util.concurrent.ConcurrentHashMap Memory Corruption	CVE: 2013-2426 BID: 59206	This strike exploits a memory corruption vulnerability in Oracle Java. The vulnerability is due to insufficient validation of serialized ConcurrentHashMap objects. Successful exploitation of this vulnerability could result in the execution of arbitrary Java code on the target system.
Strike Oracle Java sun.awt.image.ImagingLib.lookupByteBI Buffer Overflow	CVE: 2013-2463 BID: 60655	This strike exploits a buffer overflow vulnerability on the Oracle Java applet image rendering library. The vulnerability can be triggered due to improper input validation when calling the lookupByteBi function contained in the ImagingLib library. A user could be manipulated into accessing a web page that downloads and executes a malicious applet that can lead to arbitrary code execution with local user privileges.
Strike Oracle Java ImagingLib lookupByteBI Buffer Overflow	CVE: 2013-2470 BID: 60651	This strike exploits a buffer overflow vulnerability on the Oracle Java applet image rendering library. The vulnerability can be triggered due to inadequate memory management when calling the lookupByteBi function contained in the ImagingLib library. A user could be manipulated into accessing a web page that downloads and executes a malicious applet that can lead to arbitrary code execution with local user privileges.
Strike Oracle Java sun.awt.image.ByteComponentRaster Memory Corruption	CVE: 2013-2473 BID: 60623	This strike exploits a buffer overflow vulnerability on the Oracle Java applet image rendering library. The vulnerability can be triggered due to inadequate memory management when manipulating a ByteComponentRaster object with specific methods inside the AlphaComposite class. A user could be manipulated into accessing a web page that downloads and executes a malicious applet that can lead to arbitrary code execution with local user privileges.
Strike Digium Asterisk HTTP Post Request Content Length Resource Exhaustion	CWE: 119  CVE: 2013-2686  BID: 58756	This strike exploits a resource exhaustion vulnerability in Digium Asterisk. When receiving an HTTP POST request to certain URLs, Asterisk HTTP management interface allocates a heap buffer of Content-Length + 1. An attacker could send specially crafted messages with large Content-Length values to exhaust heap memory. Successful exploitation could lead to a denial of service condition.
Strike WellinTech Multiple Products ActiveX ProjectURL Property Insecure Library Loading	CWE: 94  CVE: 2013-2827  BID: 64941	This strike exploits a dll hijacking vulnerability in multiple WellinTech products. The vulnerability is due to a lack of validation of files downloaded from a source specified by the ProjectURL property of the ClientDownload ActiveX control. By enticing a user to open a crafted web page an attacker could download and execute a file from a remote location.
Strike Microsoft Internet Explorer CMarkup ElementRelease Use After Free	CWE: 119  CVE: 2013-3114  BID: 60384	This strike exploits a use after free vulnerability in Microsoft Internet Explorer. In order to exploit this vulnerability, first a DOM object must be assigned an attribute using createAttribute or setAttributeNode. The object assigned the attribute is then destroyed. If any references to the attribute still exist, any remaining references to the attribute could be accessed to create a use-after-free condition. Successful exploitation can result in execution of arbitrary code with user privileges or abnormal termination of Internet Explorer.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft IE CFlatMarkupPointer Object Handling Use-after-free	CWE: 119 CVE: 2013-3184 BID: 61668	This strike exploits a memory corruption vulnerability in Microsoft Windows Internet Explorer. The vulnerability lies in the modification of content-editable objects during onmove events. By enticing a user to view a malicious web page, an attacker could execute arbitrary code on the victim machine in the context of the user.
Strike phpMyAdmin preg_replace_php_code_execution	CVE: 2013-3238 BID: 59460	This strike exploits a code execution vulnerability in phpMyAdmin. A specially crafted HTTP POST message can be used to send arbitrary php code to the server. Successful exploitation can result in execution of the arbitrary php code with privileges of the HTTP server.
Strike Adobe ColdFusion filename Directory Traversal	CVE: 2013-3336 BID: 59773	Adobe ColdFusion contains a directory traversal vulnerability. The flaw is due to a lack of input validation by download.cfm. A remote unauthenticated attacker could exploit this vulnerability to retrieve arbitrary files, including the password file for the ColdFusion administration console.
Strike Airlive IP Camera Cross Site Request Forgery	CWE: 352 CVE: 2013-3540	This strike identifies a vulnerability in Airlive IP Cameras Web Interface. Specifically a malicious user can alter the parameters of the web interface by sending modified GET requests to the target allowing for a variety of commands to be executed that are normally not allowed. By taking advantage of the vulnerability in the usrgrp.cgi parameter in this strike we are able to create users with administrator privelages.
Strike Linksys WRT110 Command Injection vulnerability	BID: 61151 CVE: 2013-3568	This strike exploits a vulnerability inside the Linksys WRT100 and WRT110 home routers. It is possible for an authenticated remote attacker to execute arbitrary commands on a system by manipulating the arguments to the ping.cgi script.
Strike Samsung DVR Authentication Bypass	CWE: 255 CVE: 2013-3585	This strike identifies a vulnerability in Samsung DVR Firmware v1.10. An authentication bypass is possible because of improper validation of CGI page requests. If an HTTP request is made to one of many URI paths with a malicious cookie value set, then access will be given to the attacker with the ability to perform many functions such as read usernames and passwords, create users, and read and modify device configuration settings.
Strike SuperMicro IPMI login.cgi Buffer Overflow	CWE: 119 CVE: 2013-3607	This strike exploits a buffer overflow vulnerability in SuperMicro IPMI versions prior to SMT_X9_315. The vulnerability is caused by the unsafe usage of strcpy when copying to local buffers in login.cgi. A remote, unauthenticated attacker could exploit this by sending a crafted request, possibly obtaining code execution on the machine.

Name	References	Description
Strike SuperMicro IPMI close_window.cgi Buffer Overflow	CWE: 119 CVE: 2013-3623 BID: 63775	This strike exploits a buffer overflow vulnerability in SuperMicro IPMI versions prior to SMT_X9_315. The vulnerability is caused by the unsafe usage of strcpy when copying to local buffers in close_window.cgi. A remote, unauthenticated attacker could exploit this by sending a crafted request, possibly obtaining code execution on the machine.
Strike Airlive IP Camera List Parameter Information Disclosure	CWE: 264 CVE: 2013-3686	This strike identifies a vulnerability in Airlive IP Cameras. Specifically an attacker can send a malicious request to the target by means of operator/param, which will then disclose restricted information like the administrator password.
Strike Monkey HTTPD Server 1.1.1 Denial of Service	CWE: 20 CVE: 2013-3724	This Strike exploits a denial of service vulnerability in Monkey HTTPD Server version 1.1.1. When sending a request to the vulnerable service listening on port 2001 with a null byte embedded within the URI a segmentation fault occurs.
Strike Oracle Endeca Server createDataStore SOAP Request Command Execution	CVE: 2013-3763 BID: 61217	This strike exploits a command execution vulnerability in Oracle Endeca Server. A specially crafted SOAP request with the createDataStore tag can be used to execute arbitrary commands on the target system with system privileges.
Strike Oracle BPEL Process Manager BPELConsole Directory Traversal	CVE: 2013-3828 BID: 63058	This strike exploits a directory traversal vulnerability in Oracle BPEL Process Manager. GET requests to BPELConsole are not sanitized for directory traversal characters. A specially crafted GET request can be sent to access arbitrary javascript files. Successful exploitation could result in information disclosure.
Strike Microsoft .NET Framework XML XXE DOS	CWE: 20 CVE: 2013-3860 BID: 62820	This strike exploits a denial of service vulnerability in Microsoft .NET Framework. This vulnerability is due to improper handling XML files. A remote attacker can take advantage of this vulnerability to gain arbitrary files on the target system.
Strike Microsoft InformationCardSigninHelper ActiveX Remote Code Execution	CWE: 119 CVE: 2013-3918	This strike exploits a memory corruption associated with the icardie.dll dynamic library in Microsoft Windows. If a user opens a specially crafted web page where a InformationCardSigninHelper ActiveX control is instantiated, on a vulnerable machine, a memory corruption may be triggered that can lead to arbitrary code execution using local privileges. All versions of Microsoft Windows and Microsoft Windows Server are affected by this vulnerability.
Strike Squid HTTP Host Header Denial of Service	CWE: 20 CVE: 2013-4123	This strike exploits a vulnerability in Squid Internet Proxy application. If an HTTP request is received, squid parses the host headers looking for a hostname:portnumber. The port number is then used in a conversion, and if this conversion fails the process will terminate.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike SpringSource Spring Framework XEE disclosure	CWE: 264 CVE: 2013-4152 BID: 61951	This strike exploits an information disclosure vulnerability in SpringSource Spring Framework XEE disclosure. This vulnerability is due to improper handling XML files. A remote attacker can take advantage of this vulnerability to gain arbitrary files on the target system.
Strike Apache Roller OGNL Injection Remote Code Execution	CWE: 94 CVE: 2013-4212 BID: 63928	This strike exploits a security vulnerability which allows for code execution inside apache roller. The exploit provides remote unauthenticated users with command execution on the target system
Strike Nginx Request URI Verification Security Bypass	CWE: 264 CVE: 2013-4547	This strike exploits a security verification bypass flaw inside NGINX engine which takes place when incorrectly validating input from a request following a space character. The vulnerability can lead to information disclosure
Strike Netgear ProSafe startup-config Information Disclosure	CWE: 200 CVE: 2013-4775 BID: 63646	This strike exploits an information disclosure vulnerability in Netgear ProSafe. An HTTP GET request to /filesystem/startup-config will return various startup configuration details, including administrator credentials.
Strike Netgear ProSafe GET filesystem denial of service	CVE: 2013-4776 BID: 61924	This strike exploits a denial of service vulnerability in Netgear ProSafe devices. An HTTP GET request to / filesystem/ with no content will cause the device to restart or crash. Repeated requests can result in a denial of service condition.
Strike HP LoadRunner directory disclosure	CVE: 2013-4798 BID: 61443	This strike exploits a HP LoadRunner ActiveX control directory traversal vulnerability which is due to bad input sanitization of file name. Remote attackers may do arbitrary code execution on the target system.
Strike HP Intelligent Management Center BIMS UploadServlet Lack of Authentication and Directory Traversal	CVE: 2013-4822 BID: 62895	This strike exploits a lack of authentication and directory traversal vulnerability in HP Intelligent Management Center. PUT requests sent to UploadServlet are not authenticated. Furthermore, UploadServlet does not sanitize directory traversal characters. Successful exploitation can result in upload of arbitrary files in arbitrary locations, including upload of executable files or overwrite of system files.
Strike HP Intelligent Management Center BIMS bimsDownload Information Disclosure	CVE: 2013-4823	This strike exploits a command injection vulnerability inside Oracle's Secure Backup Administration web interface. The vulnerability allows command injection by passing malicious URL encoded parameters ("other") to php scripts.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike HP euAccountService Servlet Authentication Bypass Vulnerability	CWE: 287 CVE: 2013-4824 BID: 62902	This strike exploits an authentication bypass vulnerability in HP Intelligent Management Center. The vulnerability is failure to properly authenticate HTTP requests by the euAccountService servlet. A remote, unauthenticated user can exploit the vulnerability to create arbitrary web administration accounts, allowing access to all managed devices and users.
Strike HP Intelligent Management Center SOM sdFileDownload Information Disclosure	CWE: 200 CVE: 2013-4826 BID: 62898	This strike exploits a information disclosure vulnerability inside HP Intelligent Management Center SOM that can be triggered by sending malicious HTTP requests. The request can be crafted to traverse directories and as such access any file on disk.
Strike HP SiteScope issueSiebelCmd SOAP Request Handling Vulnerability	CVE: 2013-4835 BID: 63478	This strike exploits a command execution vulnerability in HP SiteScope. The vulnerability is due to authentication failure when handling issueSiebelCmd SOAP requests. Remote, unauthenticated users could execute arbitrary code simply by sending a malicious SOAP request.
Strike HP LoadRunner Virtual User Generation Emulation Directory Traversal	CVE: 2013-4837	This strike exploits two vulnerabilities inside HP LoadRunner that allow directory traversal which in turn can lead to unauthenticated arbitrary code execution or unauthenticated information disclosure
Strike HP LoadRunner Virtual User Generator saveCodeRuleFile Directory Traversal	CVE: 2013-4838 BID: 63476	This strike exploits a vulnerability in HP LoadRunner software suite . A flaw in authorization on the Virtual User Generator component could allow a remote unauthenticated attacker to delete or modify the contents of any file on the machine running the vulnerable software with elevated privileges.
Strike Sophos Web Appliance command execution	CWE: 78 CVE: 2013-4983 BID: 62263	This strike exploits a vulnerability in the Sophos Web Appliance. Due to improper input validation an unauthenticated user may execute commands on the operating system using the web interface. All versions of the Sophos Web Appliance before 3.7.9.1 and 3.8 before 3.8.1.1 are vulnerable to this attack.
Strike Symantec Endpoint Protection XXE Injection	CVE: 2013-5014 BID: 65466	This strike exploits an XXE injection vulnerability in Symantec Endpoint Protection management console. This vulnerability is due to improper handling XML external entities in the management console. A remote attacker can take advantage of this vulnerability to do DoS attack on the target system.
Strike National Instruments ABB CWGraph3D ActiveX Arbitrary File Creation	CWE: 22 CVE: 2013-5022 BID: 61282	This strike exploits an arbitrary file creation vulnerability in 3D Graph ActiveX control. The flaw is due to a lack of input validation by the 'ExportStyle' method. An attacker could exploit this vulnerability by enticing a target user to view a specially crafted web page.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Scripting Dictionary Runtime Object Library Use After Free	CWE: 416 CVE: 2013-5056	This strike exploits a use after free error triggered because of an error Microsoft Scripting Runtime Object Library . If a user opens a specially crafted web page, on a vulnerable machine, a use after free memory corruption is triggered that can lead to arbitrary code execution using local privileges. All versions of Microsoft Windows are vulnerable to this attack.
Strike Graphite Web Remote Code Execution	CWE: 94 CVE: 2013-5093 BID: 61894	This strike exploits a remote code execution vulnerability in the renderLocalView function of Graphite web versions .9.5 through .9.10. The vulnerability lies in the way that it uses the Python Pickle module.
Strike TP-Link TL-WR740N Wireless Router DoS	CWE: 134 CVE: 2013-5135	This strike exploits a vulnerability inside TP-Link TL-WR740N wireless routers that can cause a denial of service attack. The vector for attack is represented by an improper parsing process for http requests. The attack can be triggered without authentication
Strike IBM Platfor Symphony SOAP Request Processing Buffer Overflow	CWE: 119 CVE: 2013-5387 BID: 63517	This strike exploits a vulnerability in IBM Symphony cluster computing platform and SDK. Due to improper bounds validation, a remote unauthenticated attacker can send a specially crafted SOAP request causing a buffer overflow condition that can lead to DOS conditions. All versions of IBM Symphony prior to 5.2 and 6.1.x are vulnerable.
Strike IBM Rational Focal Point Login Information Disclosure	CVE: 2013-5397 BID: 64338	This strike identifies a vulnerability in IBM Rational's Focal Point. Specifically the vulnerability occurs when a request is made to the Login servlet. Requests sent to this URI are not properly validated, and xml configuration files can be disclosed to a remote unauthenticated user.
Strike IBM Rational Focal Point Information Disclosure	CVE: 2013-5398 BID: 64339	This strike identifies a vulnerability in IBM Rational's Focal Point. Specifically the vulnerability occurs when a request is made to the RequestAccessController servlet. Requests sent to this URI are not properly validated, and xml configuration files can be disclosed to a remote unauthenticated user.
Strike Cisco Prime Data Center Network Manager processImageSave.jsp Arb File Upload	CWE: 78 CVE: 2013-5486 BID: 62484	This strike exploits a vulnerability inside Cisco's Prime Data Center Network Manager, which allows remote unauthenticated arbitrary file upload through an improperly validated parameter passed through a webpage.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco Prime Data Center Network Manager Download Servlet Information Disclosure	CWE: 200 CVE: 2013-5487 BID: 62483	This strike exploits a vulnerability inside Cisco's Prime Data Center Network Manager versions prior to 6.2, which allows remote unauthenticated arbitrary file information disclosure through the downloadServlet request URI.
Strike D-Link DSL-2740B Cross Site Request Forgery	CWE: 352 CVE: 2013-5730 BID: 62356	This strike exploits a cross site request forgery exploit in D-Link DSL-2740B devices. An attacker can send a malicious web page which will then use the target's credentials to change router settings, including things such as disabling the firewall or the MAC address filter.
Strike Zabbix 2.0.8 SQL Injection	CWE: 89 CVE: 2013-5743 BID: 62794	This strike exploits an SQL injection vulnerability in Zabbix versions 1.8.17, 2.0.8, 2.1.6. The vulnerability is caused by improper sanitization of user-controlled data being used inside an SQL query. In order to exploit the vulnerability, a remote attacker would send crafted requests to the httpmon.php page. Successful exploitation could lead to privilege escalation. Having admin privileges, the attacker may then use regular application functions, obtaining code execution in the context of the web service.
Strike Oracle Demantra 12.2.1 Arbitrary File Disclosure	CVE: 2013-5877 BID: 64831	This strike exploits a vulnerability inside Oracle Demantra 12.2.1 which allows an attacker to read the content of arbitrary files on the server.
Strike WordPress Complete Gallery Manager Plugin Arbitrary File Upload	CVE: 2013-5962	This strike exploits a vulnerability inside the Complete Gallery Manager Plugin for WordPress which allows remote users to upload arbitrary files to the server.
Strike D-Link router web interface backdoor	CWE: 264 CVE: 2013-6026 BID: 62990	This strike exploits a vulnerability in web interface for D-Link routers. By using a specially crafted User-Agent string a remote attacker could completely bypass authentication and execute commands on the remote device with full administrative rights. The following models are vulnerable: DIR-100, DIR-120, DI-624S, DI-524UP, DI-604S, DI-604UP, DI-604+, TM-G5240.
Strike MW6 Aztec ActiveX Control Buffer Overflow	CVE: 2013-6040	This strike exploits buffer overflow vulnerability within the MW6 Technologies ActiveX Control. This vulnerability is due to lack of boundary checking in the MW6 Technologies Aztec ActiveX Control. Remote unauthenticated attackers could exploit this vulnerability to execute arbitrary code on the target system.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike KingView ActiveX Control File Execution	CWE: 264 CVE: 2013-6128 BID: 62419	This strike exploits a KingView ActiveX control code execution vulnerability which is due to no confirmation when executing the command in the ActiveX control. Remote attackers may do arbitrary file creation on the target system.
Strike HP Service Virtualization AutoPass License Server Directory Traversal	CWE: 22 CVE: 2013-6221 BID: 67989	This strike exploits a vulnerability inside HP Service Virtualization Autopass. Which allows directory traversal due to improper validation of user supplied data. Exploitation of this vulnerability can result in bypassing of security restrictions and arbitrary code execution.
Strike Apache Solr SolrResourceLoader Directory Traversal	CWE: 22 CVE: 2013-6397 BID: 63935	This strike exploits a security vulnerability that allows directory traversal and xslt code execution inside apache Solr. The vulnerability is triggered through a improperly sanitized GET request parameter
Strike PHP OpenSSL Certificate Corruption	BID: 64225 CWE: 119 CVE: 2013-6420	This strike exploits a vulnerability in the OpenSSL extension of PHP where a malformed certificate file can lead to memory corruption.
Strike SpringSource Spring Framework XML XEE disclosure	BID: 64947 CWE: 352 CVE: 2013-6429	This strike exploits an information disclosure vulnerability in SpringSource Spring Framework XEE. This vulnerability is due to improper handling XML files. A remote attacker can take advantage of this vulnerability to gain arbitrary files on the target system.
Strike Red Hat JBoss Seam XML XEE disclosure	CWE: 200 CVE: 2013-6447 BID: 65051	This strike exploits an information disclosure vulnerability in Red Hat JBoss Seam XML XEE. This vulnerability is due to improper handling XML files. A remote attacker can take advantage of this vulnerability to gain arbitrary files on the target system.
Strike IBM Tealeaf CX testconn_host Remote Command execution	CWE: 78 CVE: 2013-6719 BID: 65984	This strike exploits a remote command execution vulnerability in IBM Tealeaf CX. An HTTP POST request with a specially crafted testconn_host parameter can be used to execute arbitrary OS commands.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Splunk Collect Directory Traversal	CWE: 22 CVE: 2013-6771 BID: 62632	This strike exploits a vulnerability inside Splunk which allows for directory traversal through improperly parsed input parameters. If exploited, as part of specific scenarios, the vulnerability could lead to arbitrary code execution.
Strike EMC CMCNE FileUploadController Arbitrary File Upload	CWE: 94 CVE: 2013-6810	This strike exploits a EMC Connectrix Manager Converged Network Edition SAN management suite. Due to improper authorization, a remote unauthenticated attacker may upload an arbitrary files through the FileUploadController servlet. All versions of the software prior to 12.0.3 are vulnerable.
Strike Synology DiskStation manager SLICEUPLOAD Remote Command Execution	CWE: 264 CVE: 2013-6955	This strike exploits a vulnerability for Synology Diskstation Manager. Specifically, the exploit targets how user input is processed and appended to files when using the SLICEUPLOAD functionality. The flaw allows an unauthenticated remote attacker to write random command to server side script files and potentially leverage arbitrary command execution. All version belonging to 4.1.x software branch are vulnerable.
Strike Apache Camel XML Entity Information Disclosure	CWE: 264 CVE: 2014-0002 BID: 65901	This strike exploits an information disclosure vulnerability in Apache Camel. XML entities with PUBLIC or SYSTEM identifiers are processed and returned. An attacker can craft a SYSTEM entity to return information on system information or a PUBLIC entity to send requests from the Camel server, possibly allowing for policy bypass.
Strike Apache Tomcat FileUpload Content-Type Header Infinite Loop	BID: 65400 CWE: 264 CVE: 2014-0050	This strike exploits a vulnerability in Apache Tomcat web server. The vulnerability is located in the Apache Common FileUpload component specifically when parsing the Content-Type header. The flaw allows an unauthenticated remote attacker to send a specially crafted HTTP request that, once received by the server will generate a DOS condition. Apache Tomcat version 7.0.0-7.0.50 are affected by this flaw
Strike SpringSource Spring Framework XML External Entity	CWE: 352 CVE: 2014-0054 BID: 66148	This strike exploits an XML External Entity vulnerability in SpringSource Spring Framework. SpringSource will accept XML External Entities from any source. A crafted XML External Entity can be used to disclose information on the target system, cause Spring Framework to exit abnormally, leading to a denial of service condition, or us the target system to make request, possibly bypassing security policy.
Strike Apache Struts ClassLoader Delegate Security Bypass	CVE: 2014-0094 BID: 65999	This strike exploits a vulnerability inside Apache Struts which can allow remote code execution by sandbox bypass.

Name	References	Description
Strike Apache HTTP Server mod_log_config DoS	CWE: 20 CVE: 2014-0098 BID: 66303	This strike targets a vulnerability inside Apache HTTP Server that causes denial of service. The attack is triggered through cookie values and can be triggered when the mod_log_config module is activated.
Strike Apache Struts CookieInterceptor ClassLoader Security Bypass	CWE: 264 CVE: 2014-0113 BID: 67081	This strike exploits a vulnerability in the Apache Struts web suite. Due to improper sanitization it is possible for a remote attacker to invoke the ClassLoader and effectively achieve arbitrary code execution. All versions before 2.3.16.2 are vulnerable to this attack.
Strike Apache Struts ClassLoader Security Bypass	CWE: 20 CVE: 2014-0114 BID: 67121	This strike exploits a security bypass vulnerability in Apache Struts. An attacker can send crafted HTTP requests to manipulate the Java ClassLoader. Manipulation of the Java Classloader can be further exploited to achieve arbitrary code execution.
Strike Apache mod_proxy Denial of Service	CWE: 20 CVE: 2014-0117 BID: 68740	This strike exploits a denial of service vulnerability inside Apache web server. The vulnerability exists due to improper parsing of crafted Connection HTTP headers when Apache is ran using the mod_proxy module in reverse proxy mode.
Strike Apache HTTP Server mod_status Race Condition Heap Buffer Overflow, verified	CWE: 362 CVE: 2014-0226 BID: 68678	This strike exploits a race condition vulnerability in Apache HTTP Server which leads to a heap buffer overflow. When simultaneously processing requests to server-status and to any other uri, it is possible for a non-null terminated string to be created. The system attempts to copy this until it finds null characters, leading to a heap buffer overflow. Successful exploitation can result in execution of arbitrary code or abnormal termination of the Apache HTTP Server.
Strike Microsoft Direct2D API SVG Path Tag Memory Corruption	BID: 65393 CWE: 119 CVE: 2014-0263	This strike exploits a memory corruption vulnerability in the Microsoft Direct2D API. If Internet Explorer encounters an SVG Path tag that has coordinate values that are too large, memory gets corrupted and a denial of service condition will occur.
Strike Microsoft XML Core Services transformNode Information Disclosure	CWE: 200 CVE: 2014-0266 BID: 65407	This strike exploits an information disclosure vulnerability in Microsoft XML Core Services. A specially crafted web page with a certain activeX control and a specially crafted xml object can be used to return information about arbitrary files on the target system.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Scripting Runtime Object Library Use After Free	BID: 65395 CWE: 119 CVE: 2014-0271	This strike exploits a use after free error triggered because of an error Microsoft Scripting Runtime Object Library . If a user opens a specially crafted web page, on a vulnerable machine, a use after free memory corruption is triggered that can lead to arbitrary code execution using local privileges. All versions of Microsoft Windows are vulnerable to this attack.
Strike Microsoft Internet Explorer Use After Free	BID: 65372 CWE: 119 CVE: 2014-0274	This strike exploits a vulnerability in Microsoft Internet Explorer. If a DOMNodeRemoved event is triggered and all the objects that belong to the current HTMLSelection object are removed inside the event handler for DOMNodeRemoved, a use-after-free condition can occur.
Strike Microsoft Internet Explorer CSS dir rtl Memory Corruption	CWE: 119 CVE: 2014-0278 BID: 65377	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer. When specially crafted CSS style content is dynamically changed to right-to-left, an uninitialized object is accessed, leading to memory corruption. Successful exploitation may result in execution of arbitrary code or abnormal termination of Internet Explorer.
Strike Microsoft IE CInput Use-after-free Vulnerability	CWE: 119 CVE: 2014-0282 BID: 67862	This strike exploits a use-after-free vulnerability in Microsoft Internet Explorer (IE). The vulnerability is triggered when an attempt is made to access a previously deleted CInput object. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.
Strike Microsoft IE SVG HTML Content Use-after-free Vulnerability	CWE: 119 CVE: 2014-0283 BID: 65382	This strike exploits a remote code execution vulnerability in Microsoft Internet Explorer (IE). The vulnerability occurs when Internet Explorer attempts to access a previously freed SVG clipPath object. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.
Strike Microsoft Internet Explorer SelectAll appendChild Use After Free	CWE: 119 CVE: 2014-0287 BID: 65386	This strike exploits a use after free vulnerability in Microsoft Internet Explorer. A specially crafted webpage which uses 1) the document.write function in a DOM onmove or onresize event, as well as 2) a SelectAll command and 3) the DOM appendChild method can be used to trigger the vulnerability. Successful exploitation can result in execution of arbitrary code or abnormal termination of Internet Explorer.
Strike Microsoft IE Behavior URL Use-after-free Vulnerability	CWE: 119 CVE: 2014-0303 BID: 66028	This strike exploits a use-after-free vulnerability in Microsoft Internet Explorer (IE). The vulnerability is triggered when an attempt is made to access a previously deleted object while processing behavior behavior properties within an html body element. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.

Name	References	Description
Strike Microsoft Internet Explorer Use After Free CVE 2014-0305	CWE: 119 CVE: 2014-0305 BID: 66030	This strike exploits a use after free error triggered when Microsoft Internet Explorer handles DOM rewrites when processing certain web pages. If a user opens a specially crafted web page, on a vulnerable machine, a heap memory corruption is triggered that can lead to arbitrary code execution using local privileges. All versions of Internet Explorer 6 through 11.
Strike Microsoft IE TextRange Object Handling Use-After-Free Vulnerability	CWE: 119 CVE: 2014-0307 BID: 66032	This strike exploits a use-after-free vulnerability in Microsoft Internet Explorer (IE). The vulnerability lies in the handling of TextRange object. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.
Strike Adobe Flash SharedObject Use After Free	CWE: 399 CVE: 2014-0502 BID: 65702	This strike exploits a Use After Free vulnerability on Adobe Flash Player. The vulnerability can be triggered due to inadequate memory management when using a SharedObject entities. A user could be manipulated into accessing a web page that downloads and executes a malicious file that can lead to arbitrary code execution with local user privileges. All versions of flash player below 12.0.0.44 and 11.2.202.341 are affected.
Strike Novell GroupWise FileUploadServlet Directory Traversal	CWE: 200 CVE: 2014-0600 BID: 69424	This strike exploits a directory traversal vulnerability in Novell GroupWise. The vulnerability is due to improper validation of user supplied parameters in the fileUpload servlet. An unauthenticated attacker can exploit this vulnerability by sending a specially crafted request to the vulnerable server, leading to the disclosure and destruction of files in arbitrary locations on the server. NOTE: By default the vulnerable services are accessed via SSL connection (port 9710).
Strike Attachmate Reflection FTP Client ActiveX GetGlobalSettings Memory Corruption	CWE: 94 CVE: 2014-0603	This strike exploits an ActiveX control vulnerability associated with the AttachMate EXTRA!, INFOConnect and Reflection software suites. If a user opens a specially crafted web page, by instantiating a specialized ActiveX control, a memory corruption vulnerability may occur that could lead to code execution. All versions of Attachmate INFOConnect Enterprise prior to 9.2.0.1182 or Attachmate Reflection FTP Client prior to 4.1.420.0 are vulnerable.
Strike Cross-Site Scripting Vulnerability In Novell GroupWise WebAccess	CWE: 79 CVE: 2014-0611 BID: 76008	This strike exploits a cross-site scripting vulnerability in Novell GroupWise WebAccess. The vulnerability is due to improper validation while processing email attachments. An attacker could exploit this vulnerability in order to run malicious scripts on the target machine.
Strike Advantech WebAccess SCADA webvact.ocx GotoCmd Buffer Overflow	CWE: 119 CVE: 2014-0765 BID: 66722	This strike exploits a security vulnerability inside Advantech WebAccess which can lead to remote code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Advantech WebAccess SCADA webvact NodeName2 Buffer overflow	CWE: 119 CVE: 2014-0766 BID: 66725	This strike exploits a buffer overflow vulnerability inside Advantech WebAccess SCADA which can lead to arbitrary code execution in the context of the logged in user.
Strike Advantech WebAccess SCADA webvact AccessCode Buffer overflow	CWE: 119 CVE: 2014-0767 BID: 66728	This strike exploits a buffer overflow vulnerability inside Advantech WebAccess SCADA which can lead to arbitrary code execution in the context of the logged in user.
Strike Advantech WebAccess SCADA webvact AccessCode2 Buffer overflow	CWE: 119 CVE: 2014-0768 BID: 66732	This strike exploits a buffer overflow vulnerability inside Advantech WebAccess SCADA which can lead to arbitrary code execution in the context of the logged in user.
Strike Advantech WebAccess BWOXRUN.Bwocxr unCtrl ActiveX Code Execution vulnerability	CVE: 2014-0773 BID: 66742	This strike exploits a remote code execution vulnerability in Advantech WebAccess. The vulnerability lies within the CreateProcess method used by the bwocxrun.ocx ActiveX Control. By enticing a user to open a crafted web page an attacker could remotely execute arbitrary code.
Strike IBM SPSS Sample Power Vsflex8l Combolist Buffer Overflow	CWE: 119 CVE: 2014-0895 BID: 66116	This strike targets a vulnerability inside IBM SPSS SamplePower that exist due to improper boundary checking and which could lead to code execution in the context of the user targeted by the attack. The attack is carried out through Vsflex8l ActiveX control
Strike WordPress WP Symposium Plugin Arbitrary File Upload	CVE: 2014-10021 BID: 71686	This strike exploits a file upload vulnerability in Wordpress WP Symposium Plugin version 14.11. The vulnerability is due to lack of sanitization of the user-uploaded files in UploadHandler.php. By exploiting this vulnerability, an unauthenticated attacker can execute arbitrary code by uploading files on the server and execute them.
Strike SOAPUI Remote Code Execution	CWE: 94 CVE: 2014-1202	This strike exploits a vulnerability inside the SOAPUI testing suite. Specifically, if a user is tricked into accessing a specially formatted WSDL document, local code execution may be achieved. All versions of SOAPUI prior to 4.6.4 are affected.

Name	References	Description
Strike Mozilla Firefox TypeObject Use After Free	CWE: 399 CVE: 2014-1512 BID: 66209	This strike exploits a use after free vulnerability in Mozilla Firefox. The vulnerability occurs while handling TypeObjects within the JavaScript engine. By enticing a user to view a malicious web page, an attacker could execute arbitrary code on the victim's machine.
Strike Mozilla Firefox SharedWorker Port Close Use After Free	CVE: 2014-1548 BID: 68818	This strike exploits a use after free vulnerability in Mozilla Firefox. If a SharedWorker is created then has its MessagePort closed, the pointer is left but the object is removed by the garbage collector. The dangling pointer can be accessed, creating a use after free condition.
Strike Mozilla Firefox SVG Animation Use After Free	CWE: 416 CVE: 2014-1563 BID: 69523	This strike exploits a Use After Free vulnerability in Mozilla Firefox. The vulnerability is due to a flaw in the handling of SVG objects embedded in web pages. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, leading to execution of arbitrary code on the victim system.
Strike CenturyStar ActiveX Control SetMyAddress BO	CWE: 787 CVE: 2014-1598	This strike exploits buffer overflow vulnerability within CenturyStar 7.12 ActiveX Control. This vulnerability is due to lack of boundary checking in the CenturyStar 7.12 ActiveX Control. Remote unauthenticated attackers could exploit this vulnerability to execute arbitrary code on the target system.
Strike Belkin N750 DB Wi-Fi Gigabit Router Buffer Overflow	CWE: 119 CVE: 2014-1635 EXPLOITDB : 35184 BID: 70977	This strike exploits a buffer overflow vulnerability inside Belkin's N750 DB Wi-Fi router. If exploited the vulnerability results in command execution in the context of the root user which effectively grants full access of the device to the attacker.
Strike Mitsubishi EZPcAut260.dll ActiveX Control ESOOpen Buffer Overflow	CVE: 2014-1641	This strike exploits buffer overflow vulnerability within Mitsubishi EZPcAut260.dll ActiveX Control. This vulnerability is due to lack of boundary checking in the function ESOOpen in Mitsubishi EZPcAut260.dll ActiveX Control. Remote unauthenticated attackers could exploit this vulnerability to execute arbitrary code on the target system.
Strike Symantec LiveUpdate Administrator Security Bypass	CWE: 255 CVE: 2014-1644 BID: 66399	This strike identifies a security policy bypass vulnerability in Symantec LiveUpdate Administrator. When processing a Post request, the temporary passwords are not properly validated allowing for a malicious user to take advantage of the reset old password feature to force a reset and create user account information.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Symantec Workspace Streaming xmlrpc ManagementAgentServer Arbitrary File Upload	CWE: 264 CVE: 2014-1649 BID: 67189	This strike exploits an arbitrary file upload vulnerability in Symantec Workspace Streaming. An attacker can send a specially crafted HTTP POST message with an XML_RPC call to ManagementAgentServer to upload an arbitrary file onto the target. Successful exploitation could result in arbitrary file creation or file overwrite.
Strike Symantec Web Gateway clientreport.php SQL Injection	CWE: 89 CVE: 2014-1651 BID: 67754	This strike exploits an SQL injection vulnerability in Symantec Web Gateway management console versions prior to 5.2. The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure, database corruption, denial of service and others.
Strike SkyBlueCanvas CMS Un-Authenticated Command Execution	CWE: 134 CVE: 2014-1683 BID: 65129	This strike identifies a vulnerability in SkyblueCanvas CMS that allows for command execution by sending a request to the vulnerable CMS application. The parameters "name", "email", "subject", and "message" are not properly validated, therefore allowing an unauthenticated user to issue malicious commands.
Strike Google Chrome V8 Javascript ArrayBuffer Memory Corruption Vulnerability	CWE: 119 CVE: 2014-1705 BID: 66239	This strike exploits a memory corruption vulnerability in Google Chrome. The vulnerability can be exploited by overwriting a function for accessing a TypedArray property. By enticing a user to open a malicious web page, an attacker could exploit this vulnerability to execute arbitrary code on the client system.
Strike Microsoft IE removeAttribute Use-after-free Vulnerability	CWE: 399 CVE: 2014-1765 BID: 66244	This strike exploits a use-after-free vulnerability in Microsoft Internet Explorer (IE). The vulnerability is triggered when an attempt is made to access a previously deleted style attribute. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.
Strike Microsoft Internet Explorer Object OnError CTreePos Use After Free	CWE: 119 CVE: 2014-1772 BID: 67864	This strike exploits a use after free vulnerability in Microsoft Internet Explorer. The vulnerability is caused by improper management of resources during event handling by the Internet Explorer engine. A remote attacker could entice the user to access a crafted HTML page, potentially obtaining code execution in the context of the user accessing the page.
Strike Microsoft Internet Explorer PushClipRect Array Indexing Memory Corruption	CWE: 119 CVE: 2014-1773 BID: 67866	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer. An attacker can entice a target to visit an HTML page with a specially crafted canvas object to trigger the vulnerability. Successful exploitation can result in execution of arbitrary code or abnormal termination of Internet Explorer.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer CPeerFactoryUrlMap Use-after-free Vulnerability	CWE: 119 CVE: 2014-1775 BID: 67871	This strike exploits a use-after-free vulnerability in Microsoft Internet Explorer (IE). The vulnerability is triggered when attempting to access a deleted CPeerFactoryUrlMap object. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.
Strike Microsoft IE VML Object Handling Use-After-Free Vulnerability	CWE: 416 CVE: 2014-1776 BID: 67075	This strike exploits a use-after-free vulnerability in Microsoft Internet Explorer (IE). The vulnerability lies in the handling of VML groups. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.
Strike Internet Explorer replaceNode Memory Corruption	CWE: 119 CVE: 2014-1789 BID: 67881	This strike exploits a Memory Corruption vulnerability in Internet Explorer. The vulnerability is due to error while dynamically replacing DOM nodes. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.
Strike CVE-2014-1791 Microsoft Internet Explorer Memory Corruption	CWE: 119 CVE: 2014-1791 BID: 67884	This strike exploits a use after free memory corruption vulnerability inside Microsoft Internet Explorer. The vulnerability can be triggered by enticing a user to access a malicious website and could result in remote code execution. If code execution is achieved, it will be run in the context of the user.
Strike Microsoft Internet Explorer createTextRange Page Hide Use After Free	CWE: 119 CVE: 2014-1795 BID: 67887	This strike exploits a use after free vulnerability in Microsoft Internet Explorer. The createTextRange command creates a CMarkup object. This object gets deleted on page hide. The onpagehide command can execute calls on page hide, including manipulating the deleted CMarkup object, causing a use after free condition. Successful exploitation may result in execution of arbitrary code or abnormal termination of Internet Explorer.
Strike Microsoft Internet Explorer Marquee Object Use After Free	CWE: 119 CVE: 2014-1815 BID: 67301	This strike exploits a Use-After-Free vulnerability in Microsoft Internet Explorer. The vulnerability is due to an error while handling marquee objects within HTML pages. By enticing a user to view a malicious web page, an attacker could execute arbitrary code on the victim's machine.
Strike Mitsubishi EZPcAut220 ActiveX Control HostAddress Buffer Overflow	CVE: 2014-1847	This strike exploits buffer overflow vulnerability within Mitsubishi EZPcAut220.dll ActiveX Control. This vulnerability is due to lack of boundary checking in the attribute HostAddress in Mitsubishi EZPcAut220.dll ActiveX Control. Remote unauthenticated attackers could exploit this vulnerability to execute arbitrary code on the target system.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Schneider Electric ClearSCADA 2013R1.2 GetOPCServers ActiveX Control BO	CVE: 2014-1848	This strike exploits buffer overflow vulnerability within Schneider Electric ClearSCADA 2013R1.2 ActiveX Control. This vulnerability is due to lack of boundary checking in the Schneider Electric ClearSCADA 2013R1.2 ActiveX Control. Remote unauthenticated attackers could exploit this vulnerability to execute arbitrary code on the target system.
Strike Mitsubishi ActiveX Control EZPcAut280.dll KeywordSet Argument Buffer Overflow	CVE: 2014-2074	A buffer overflow vulnerability exists in Mitsubishi ActiveX Control EZPcAut280.dll. The vulnerability is due to a boundary error in while parsing arguments passed to the KeywordSet argument.
Strike CA ERwin Web Portal ProfileIconServlet Directory Traversal	CWE: 22 CVE: 2014-2210 BID: 66644	This strike exploits a directory traversal vulnerability in CA ERwin Web Portal. The parameters fileName and customImageName are not sanitized for directory traversal characters in requests to ProfileIconServlet. Successful exploitation can result in disclosure of arbitrary files.
Strike Vtiger CRM Unauthenticated Password Reset	CWE: 20 CVE: 2014-2269 BID: 66757	This strike identifies a vulnerability in Vtiger's web-based Customer Relationship Management system. Due to a lack of user restriction on the changePassword function an unauthenticated user can alter the password of the administrator account.
Strike PHP Libmagic Executable PE Selection Table Entry Out of Bounds Memory Access	CWE: 119 CVE: 2014-2270	This strike exploits an out of bounds memory access vulnerability in PHP Libmagic. An executable file with a specially crafted PE selection table entry can cause an integer overflow when calculating the memory address. This will bypass verification, allowing for access of an out of bounds memory location. Successful exploitation can result in execution of arbitrary code or abnormal termination of PHP, resulting in a denial of service condition.
Strike EMC CMCNE FileUploadController FILELOCATION Directory Traversal	CWE: 264 CVE: 2014-2276 BID: 66308	This strike exploits a directory traversal vulnerability in EMC Connectrix Manager Converged Network Edition (CMCNE). CMCNE does not sanitize "../" in the FILELOCATION header in requests to /inmservlets/FileUploadController for directory traversal characters. A specially crafted HTTP request can be sent to gain access to files normally not accessible.
Strike Digium Asterisk Cookie Stack Overflow CVE-2014-2286	CWE: 20 CVE: 2014-2286 BID: 66093	This strike exploits a vulnerability inside Digium Asterisk that allows stack overflow through the Cookie header inside HTTP GET requests. This vulnerability could be leveraged conduct denial of service attacks

Name	References	Description
Strike Atlassian Jira Issue Collector Directory Traversal	CWE: 22 CVE: 2014-2314 BID: 65849	This strike exploits a vulnerability in the Atlassian JIRA software suite. It allows a remote unauthenticated attacker to upload a file to random location on the file system by exploiting a directory traversal vulnerability. All versions of JIRA prior to 6.0.3 are vulnerable.
Strike ZTE F460-F660 cable modem web_shell_cmd.gch Command Injection	CWE: 264 CVE: 2014-2321	This strike exploits a command execution vulnerability in ZTE F460/F660 cable modem Web Interface. The vulnerability is due to improper access checks of the web platform resources. Successful exploitation can result in arbitrary commands on the target system.
Strike Lighttpd Host Header mod_simple_vhost directory traversal	CWE: 22 CVE: 2014-2324 BID: 66157	This strike exploits a vulnerability in the Lighttpd Web Server. Due to insufficient input validation, a malicious user may send a request with a specially crafted Host header and generate a directory traversal. All versions of Lighttpd Project Lighttpd prior to 1.4.35 are vulnerable.
Strike Oracle Data Quality PostcardPreviewInt Onclose Untrusted Pointer Dereference	CVE: 2014-2415	This strike exploits an untrusted pointer dereference vulnerability inside Oracle Data Quality. The vulnerability can be exploited to gain arbitrary code execution on the target system in the context of the logged in user.
Strike Oracle Data Quality DateTimeWrapper onchange Untrusted Pointer Dereference	CVE: 2014-2416	This strike exploits a pointer dereference vulnerability inside Oracle Data Quality. The vulnerability could provide attackers with remote code execution in the security context of the logged in user.
Strike Oracle Data Quality onloadstatechange Pointer Dereference	CVE: 2014-2417 BID: 66841	This strike exploits a pointer dereference vulnerability in Oracle Data Quality. The onloadstatechange property of the TSS12.DscXB.XB ActiveX control expects a function and does not check type of data it is passed. Passing in a different type can result in invalid memory access. Successful exploitation may result in read/write to arbitrary memory, arbitrary code execution, or abnormal termination of the web browser.
Strike Oracle Data Quality FileChooserDlg onChangeDirectory Untrusted Pointer Dereference	CWE: 822 CVE: 2014-2418	A remote code execution vulnerability exists in Oracle Data Profiling and Data Quality for Data Integrator. The vulnerability is due to dereferencing an arbitrary pointer within the TSS12.DscTools.FileChooserDlg ActiveX control. A remote attacker can exploit this vulnerability by enticing a user to open a malicious web page. Successful exploitation could result in arbitrary code execution in the context of the currently logged on user.
Strike Oracle Event Processing FileUploadServlet filename Parameter Directory Traversal	CVE: 2014-2424 BID: 66871	This strike exploits a directory traversal exploit in Oracle Event Processing. When processing multipart messages sent to FileUploadServlet, the filename parameter is not sanitized for directory traversal characters. Successful exploitation can result in creation or overwrite of arbitrary files.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike LibYAML scanner yasml_parser_scan_uri_escapes Heap Bufferoverflow	CWE: 119 CVE: 2014-2525 BID: 66478	This strike exploits a vulnerability in the LibYAML open source library. Due to improper memory management, when handling Uri encoded tag elements, opening a specially formatted YAML file will cause a heap overflow that could potentially lead to code execution. All versions of the LibYAML library prior to 0.1.5 are vulnerable
Strike HP SiteScope EmailServlet webinfra_emailFileName Directory Traversal	CWE: 287 CVE: 2014-2614 BID: 68361	This strike exploits a directory traversal vulnerability in HP SiteScope. The webinfra_emailFileName parameter in http requests to /SiteScope/EmailServlet is not sanitized for directory traversal characters. A specially crafted HTTP request can be sent to a vulnerable server to access information not normally accessible.
Strike HP Universal CMDB Default Credentials Arbitrary File Upload	CVE: 2014-2617 BID: 68363	This strike exploits a code execution vulnerability in HP Universal CMDB. The vulnerability is due to the use of hard-coded credentials with administrator rights. By exploiting this vulnerability, an attacker can upload files on the server using the hard-coded credentials and execute code with SYSTEM privileges.
Strike HP Intelligent Management Center Branch Intelligent Management Software Directory Traversal	CVE: 2014-2618 BID: 68540	This strike exploits a directory traversal vulnerability in HP Intelligent Management Center (IMC) Branch Intelligent Management Software (BIMS). When processing the fileName parameter in an HTTP request, BIMS does not sanitize for directory traversal characters. Successful exploitation can result in disclosure of arbitrary files on the target machine.
Strike HP Intelligent Management Center SyslogDownloadServlet Information Disclosure	CVE: 2014-2619 BID: 68543	This strike exploits a directory traversal vulnerability inside HP Intelligent Management Center which can be attacked through the SyslogDownloadServlet resource. If exploited the vulnerability could result in arbitrary file disclosure.
Strike HP Intelligent Management Center FaultDownloadServlet Information Disclosure	CVE: 2014-2620 BID: 68544	This strike exploits a vulnerability in the HP Intelligent Management Center. Due to insufficient input validation, a malicious user may send a request with a specially crafted URL that generates directory traversal conditions and may allow access to any file on the system. All versions of HP Intelligent Management Center prior to 7.0 are vulnerable.
Strike HP Intelligent Management Center ICTDownloadServlet Information Disclosure	CVE: 2014-2621 BID: 68546	This strike exploits an information disclosure vulnerability inside HP Intelligent Management Center. The vulnerability is available due to improper validation of input parameters and can be accessed through the ICTDownload servlet. If exploited the vulnerability grant read access to all files on the targeted system.
Strike HP Network Virtualization toServerObject Directory Traversal	CWE: 22 CVE: 2014-2626 BID: 68851	This strike exploits a directory traversal vulnerability inside HP Network Virtualization. The vulnerability allows arbitrary file upload on the target server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike HP Sprinter Tidestone Formula ActiveX SwapTables Memory Corruption	CVE: 2014-2635 BID: 70354	This strike exploits a memory-corruption vulnerability in an HP Sprinter ActiveX control. The vulnerability is due to a failure to sanitize user-supplied input, allowing a user to pass part of a memory address as a method parameter to the SwapTables method. By enticing a user to view a malicious web page, an attacker could execute arbitrary code on the victim system.
Strike HP Sprinter Tidestone Formula ActiveX AttachToSS Memory Corruption	CVE: 2014-2636 BID: 70358	This strike exploits a memory-corruption vulnerability in an HP Sprinter ActiveX control. The vulnerability is due to a failure to sanitize user-supplied input, allowing a user to pass part of a memory address as a method parameter to the AttachToSS method. By enticing a user to view a malicious web page, an attacker could execute arbitrary code on the victim system.
Strike HP Sprinter Tidestone Formula ActiveX Multiple Memory Corruption	CVE: 2014-2637 BID: 70357	This strike exploits a memory-corruption vulnerability in an HP Sprinter ActiveX control. The vulnerability is due to a failure to sanitize user-supplied input, allowing a user to pass part of a memory address as a method parameter to the CopyRange and CopyRangeEx methods. By enticing a user to view a malicious web page, an attacker could execute arbitrary code on the victim system.
Strike HP Sprinter Tidestone Formula One ActiveX DefaultFontName Buffer Overflow	CVE: 2014-2638	This strike exploits a flaw in HP Sprinter that results in execution of arbitrary code triggered by manipulation of object property in ActiveX controls.
Strike Microsoft Internet Explorer TextArea Use After Free	CWE: 119  CVE: 2014-2782  BID: 68101	This strike exploits a Use-After-Free vulnerability in Internet Explorer. The vulnerability is due to an attempt to use a TextArea object after it has been improperly deleted. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.
Strike Microsoft IE History Use-after-free Vulnerability	CWE: 119  CVE: 2014-2804  BID: 68386	This strike exploits a use-after-free vulnerability in Microsoft Internet Explorer (IE). The vulnerability is triggered when a modifying the browser history state. By enticing a user to view a malicious web page, an attacker can remotely execute arbitrary code.
Strike Internet Explorer CDOMUIEvent Memory Corruption	CWE: 119  CVE: 2014-2820  BID: 69116	This strike exploits a Memory Corruption vulnerability in Internet Explorer. The vulnerability is due to an error while processing events using the dispatchEvent method. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Apple CUPS Web Interface URL XSS	CWE: 79 CVE: 2014-2856 BID: 66788	This strike exploits a reflected XSS vulnerability inside CUPS which can lead to information disclosure on the target's machine. The vulnerability is present due to poor input validation inside the URL and can lead to exposure of sensitive data residing on the client, like session cookies
Strike F5 Multiple Products iControl API hostname remote command execution	CVE: 2014-2928 BID: 67278	This strike exploits a remote command execution vulnerability in multiple F5 products. The vulnerability is due to lack of validation of user supplied input in set_hostname SOAP requests. An unauthenticated remote attacker can exploit this vulnerability by sending specially crafted SOAP allowing the attacker to execute shell commands on the vulnerable server. NOTE: By default the vulnerable services are accessed via SSL connection (port 443).
Strike Belkin Router N150 Path Traversal	CWE: 22 CVE: 2014-2962 BID: 68085 EXPLOITDB : 38488	This strike exploits an absolute path traversal vulnerability in the webproc cgi module on the Belkin N150 router. This vulnerability could allow remote attackers to read arbitrary files via a full pathname in the HTTP getpage parameter.
Strike Sixnet Sixview Web Console Directory Traversal	CWE: 22 CVE: 2014-2976 BID: 67032	The strike exploits a directory traversal vulnerability inside Sixnet SixView Manager 2.4.1 that allows remote attackers to read arbitrary files by specifying traversal characters.
Strike Acunetix 8 Remote Stack Based Buffer Overflow	CWE: 119 CVE: 2014-2994 BID: 67058	This strike exploits a vulnerability inside Acunetix Web Application Vulnerability Scanner 8. The vulnerability can be exploited by supplying a specially crafted website as the scanner's target and can result in remote code execution.
Strike ElasticSearch Dynamic Script Arbitrary Java Execution Vulnerability	CWE: 284 CVE: 2014-3120 BID: 67731	This strike exploits a remote code execution vulnerability in ElasticSearch. The vulnerability is due to a design flaw allowing code execution as part of query. Exploiting this vulnerability could allow remote, unauthenticated attackers to execute arbitrary code on the target server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Symantec Endpoint Protection Manager Cross-Site Scripting Vulnerabilities	CWE: 79 CVE: 2014-3438 BID: 70844	This strike exploits one of two reflected Cross-Site Scripting (XSS) vulnerabilities in Symantec Endpoint Protection Manager. The vulnerabilities are due to improper sanitization of parameters prior to presenting content to the user. A remote attacker could exploit these vulnerabilities by enticing a user to follow a malicious link, which could result in arbitrary execution of script code. NOTE: Communication with the Javascript-based console is via HTTPS (TCP/8443)
Strike SAP Sybase Event Stream Processor XML-RPC ConnectionType Unsafe Pointer Dereference	CVE: 2014-3457 BID: 67585	This strike exploits an unsafe pointer dereference vulnerability in SAP Sybase Event Stream Processor. An HTTP POST request with a specially crafted XML-RPC command can be used to cause the program to dereference an arbitrary memory location. Successful exploitation can result in execution of arbitrary code or abnormal termination of the esp_parse service.
Strike Sybase Event Stream Processor Connection Pointer Dereference	CVE: 2014-3458 BID: 67587	This strike exploits unsafe pointer dereference vulnerabilities in SAP Sybase Event Stream Processor ESP Studio. The XML-RPC methods Connection.getErrors and Connection.getType both accept user-supplied input as pointer to a location in memory. By sending specially crafted XML-RPC commands an attacker could cause a Denial of Service condition.
Strike PHP Unserialize SplObjectStorage and ArrayObject Member Array Memory Corruption	CVE: 2014-3515 BID: 68237	This strike exploits a memory corruption vulnerability in PHP. When PHP attempts to deserialize a specially crafted serializable object a type confusion will occur, resulting in memory corruption. Successful exploitation may result in arbitrary code executions with the privileges of the PHP application or abnormal program termination.
Strike Squid Range Header Denial of Service	CWE: 20 CVE: 2014-3609 BID: 69453	This strike exploits a vulnerability in the Squid proxy which can be exploited due to improper validation of input parameters. The vulnerability can be triggered through Range headers inside the requests. The vulnerability can be exploited remotely and results in a denial of service condition.
Strike PHP Core Unserialize Calls Object Length Integer Overflow	CWE: 189 CVE: 2014-3669 BID: 70611	This strike exploits an integer overflow vulnerability in PHP. When processing serializable objects, the value of the DataLen fields of a class object is not verified. A sufficiently large DataLen value will cause an integer overflow, which may result in memory corruption. Successful exploitation may result in execution of arbitrary code with the privileges of the PHP application or abnormal termination of the PHP application, resulting in a denial of service condition.
Strike Drupal 7 Preauth SQL Injection	BID: 70595 CWE: 89 CVE: 2014-3704	This strike exploits a vulnerability in Drupal 7 versions pre 7.32 which allows malicious users to perform unauthenticated SQL injection attacks. When exploited, the vulnerability can result in complete compromise of the target website.

Name	References	Description
Strike Cogent DataHub Web Server GetPermissions Command Injection	CWE: 94 CVE: 2014-3789 BID: 67486	This strike exploits a vulnerability inside Cogent DataHub Web Server that allows an attacker to execute commands in the context of the DataHub process. The vulnerability exists due to improper validation of input parameters passed to the authenticate function
Strike Centreon and Centreon Enterprise Server SQL Injection	CWE: 89 CVE: 2014-3828 BID: 70648	This strike exploits an SQL injection vulnerability in Centreon versions 2.5.2 and prior and Centreon Enterprise Server versions 2.2 and prior, as well as 3.0. The vulnerability is caused by improper sanitization of parameters passed in requests to multiple application pages. An unauthenticated remote attacker could exploit this vulnerability by sending crafted packets to the application, resulting in the injection of SQL commands to the underlying database.
Strike Centreon and Centreon Enterprise Server Remote Command Injection	CWE: 94 CVE: 2014-3829 BID: 70649	This strike exploits a remote command injection vulnerability in Centreon versions 2.5.2 and prior and Centreon Enterprise Server versions 2.2 and prior, as well as 3.0. The vulnerability is caused by improper sanitization of the template_id and session_id parameters in displayServiceStatus.php, as well as improper escaping of a shell argument field. An attacker may resort to SQL injection on these fields in order to bypass security checks and prepare a command for subsequent execution. Successful exploitation depends upon a user (any user) being logged in to the application during the attack and will result in remote command execution.
Strike Samsung iPOLiS Device Manager FindConfigChildeKeyList Stack Buffer Overflow	CWE: 119 CVE: 2014-3912 BID: 67823	This strike exploits a Samsung iPOLiS Device Manager vulnerability which is due to improper bound validation in the FindConfigChildeKeyList method. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike Rocket Servergraph Admin Center fileRequest Arbitrary File Creation	CWE: 22 CVE: 2014-3914 BID: 67779	This strike exploits a arbitrary file creation vulnerability present in Rocket Servergraph Admin Center. The vulnerability is present due to lack of checks on user supplied data and can be exploited through the use of fileRequest resources. Successfull exploitation can result in arbitrary code execution on the target machined in the context of the SYSTEM user.
Strike Rocket Servergraph Admin Center run and runClear Command Execution	CWE: 22 CVE: 2014-3914	This strike exploits a command execution vulnerability present in Rocket Servergraph Admin Center. The vulnerability is present due to lack of checks on user supplied data and can be exploited through the use of fileRequest resource. Successful exploitation can result in arbitrary code execution on the target machined in the context of the SYSTEM user.

Name	References	Description
Strike Rocket Servergraph Admin Center userRequest and tsmRequest Command Execution	CWE: 94 CVE: 2014-3915 BID: 67780	This strike exploits a arbitrary command execution present in Rocket Servergraph Admin Center. The vulnerability is present due to lack of checks on user supplied data and can be exploited through the use of tsmRequest and userRequest resources. The command gets executed in the context of the System user.
Strike D-Link HNAP HTTP POST Content Stack Buffer Overflow	CWE: 119 CVE: 2014-3936 BID: 67651	This strike exploits a stack overflow vulnerability in multiple D-Link devices using Home Network Administration Protocol (HNAP). When processing an HNAP request, the vulnerable devices copy the request content to a fixed buffer without validating the size. Successful exploitation may result in attacker control of the vulnerable device.
Strike Multiple ManageEngine Products LinkViewFetchServlet SQL Injection	CWE: 89 CVE: 2014-3996 BID: 69305	This strike exploits a SQL injection vulnerability in multiple ManageEngine products. The vulnerability is due to improper sanitization of a parameter in LinkViewFetchServlet. By exploiting this vulnerability, an attacker can inject SQL commands and execute code on the target server.
Strike Internet Explorer first-letter element styling Memory Corruption	CWE: 119 CVE: 2014-4050 BID: 69125	This strike exploits a Memory Corruption vulnerability in Internet Explorer. The vulnerability is due to an error while handling CSS pseudo-objects. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the target machine.
Strike Microsoft Internet Explorer CSegment Use After Free	CWE: 119 CVE: 2014-4063 BID: 69132	This strike exploits a use after free vulnerability in Internet Explorer. If the style attribute function executes selectAll and the onreadystatechange event executes selectAll and indent, a CSegment object is deleted and later accessed, creating a use after free condition. Successful exploitation could result in execution of arbitrary code.
Strike Microsoft XML Core Services XML Content Parsing Memory Corruption	CWE: 94 CVE: 2014-4118 BID: 70957	This strike exploits a flaw in Microsoft XML Core Services. The vulnerability is due to an uninitialized variable while processing the value of the priority element in xsl:template. By exploiting this vulnerability, an attacker can determine arbitrary code execution.
Strike Microsoft .NET System.dll iriParsing Remote Code Execution	CWE: 399 CVE: 2014-4121 BID: 70351	This strike exploits a heap corruption vulnerability in Microsoft .NET Framework. The vulnerability is due to an integer underflow occurring while Internationalized Resource Identifier (IRI) elements are processed. A remote, unauthenticated attacker can execute arbitrary code in the context of .NET web application by sending crafted IRI strings to the vulnerable server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer onerror CTitleElement Use After Free	CWE: 20 CVE: 2014-4130 BID: 70332	This strike exploits a use after free error in Microsoft Internet Explorer. A specially crafted webpage can free and then attempt to access the MSHTML!CTitleElement Object. Successful exploitation can lead to execution of arbitrary code or abnormal termination of Internet Explorer.
Strike Microsoft Internet Explorer basefont ASLR Bypass	CWE: 264 CVE: 2014-4140 BID: 70325	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer. An attacker can entice a target to visit an HTML page with a specially crafted basefont tag to trigger the vulnerability. Successful exploitation can result in execution of arbitrary code or abnormal termination of Internet Explorer.
Strike SENKAS Kolibri Webserver Request Buffer Overflow	CWE: 119 CVE: 2014-4158 BID: 68195 EXPLOITDB : 33027	This strike exploits a buffer overflow vulnerability in Kolibri webserver. The overflow can be triggered through GET and HEAD requests and can result in remote code execution.
Strike Manage Engine Desktop Central Arbitrary File Upload	CWE: 22 CVE: 2014-5005 BID: 69494	This strike exploits a vulnerability in Manage Engine Desktop Central product which allows arbitrary file upload. The vulnerability exists due to lack of parsing of directory traversal characters.
Strike ManageEngine Desktop Central Directory Traversal	CWE: 22 CVE: 2014-5006 BID: 69493	This strike exploits a directory traversal vulnerability in ManageEngine Desktop Central. The vulnerability is due to improper validation of the filename parameter in mdmLogUploader. By exploiting this vulnerability, an attacker can upload files to arbitrary locations on the server and execute code.
Strike OSSIM AlienVault av-centerd Util.pm remote_task Arbitrary Command Execution	CWE: 94 CVE: 2014-5210 BID: 69239	This strike exploits a vulnerability in the OSSIM AlienVault software suite. By sending a specially crafted SOAP request an unauthenticated attacker can execute commands on a vulnerable system. All AlienVault versions prior to 4.7.0 are vulnerable.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Novell eDirectory rdn Parameter Cross Site Scripting	CWE: 79 CVE: 2014-5212 BID: 71741	This strike exploits a memory corruption vulnerability in Novell eDirectory. In HTTP requests to /nds/search/data, the rdn parameter is not properly sanitized. An attacker could place arbitrary script codes into the parameter, which will then be executed with the privileges of the current browser session.
Strike Drupal Core XML-RPC Excessive Parameter Tags Denial of Service	CWE: 399 CVE: 2014-5266 BID: 69146	This strike exploits a denial of service vulnerability in Drupal Core. Due to how Drupal Core parses XML, an XML-RPC request with excessive parameter tags can cause CPU and memory exhaustion, causing a denial of service condition.
Strike ManageEngine Multiple Products FileAttachment directory traversal	CWE: 22 CVE: 2014-5301	This strike exploits a directory traversal vulnerability in multiple ManageEngine products. The vulnerability is due to improper validation of the path parameter when uploading files to the server. By exploiting this vulnerability, an authenticated attacker can upload files to arbitrary locations on the server and execute them.
Strike ManageEngine Multiple Products FileCollector doPost Directory Traversal	CWE: 22 CVE: 2014-6034	This strike exploits a remote arbitrary file upload vulnerability inside ManageEngine. The vulnerability exists due to improper sanitization of input characters and can lead to arbitrary code execution in the context of the System user.
Strike Manage Engine Multiple Products File Collector Directory Traversal	CWE: 22 CVE: 2014-6035 BID: 70169	This strike exploits a vulnerability in multiple Manage Engine products which allows arbitrary file upload. The vulnerability exists due to lack of parsing of directory traversal characters.
Strike ManageEngine Multiple Products multipartRequest Directory Traversal	CWE: 22 CVE: 2014-6036 BID: 70172	This strike exploits a vulnerability inside multiple products from the Manage Engine suite which allows arbitrary file execution. The vulnerability is due to lack of authentication controls and directory traversal vulnerabilities.
Strike ManageEngine EventLog Analyzer agentUpload Directory Traversal	CWE: 22 CVE: 2014-6037 BID: 69482	This strike exploits a code execution vulnerability inside ManageEngine EventLog Analyzer. The vulnerability allows remote unauthenticated attackers to upload files to arbitrary locations and grants execution abilities with System privileges.

Name	References	Description
Strike ManageEngine EventLog Analyzer agentHandler Information Disclosure	CWE: 200  CVE: 2014-6038  BID: 70959	This strike exploits an information disclosure inside ManageEngine EventLog Analyzer. The vulnerability is exploited through the agentHandler servlet and allows remote unauthenticated information disclosure from within the databases available inside the application.
Strike ManageEngine EventLog Analyzer Hostdetails Information Disclosure	CVE: 2014-6039  BID: 70960	This strike exploits an information disclosure inside ManageEngine EventLog Analyzer. The vulnerability is exploited through the agentHandler servlet and allows remote unauthenticated information disclosure in regard to the details of the server hosting the application.
Strike Google Android Browser Same Origin Policy Bypass	CWE: 264  CVE: 2014-6041  BID: 69548	This strike exploits a vulnerability inside Google's Android browser which allows violation of the same origin policy bypass. The vulnerability can be exploited through the use of window.location property and can result in session takeover.
Strike Zenoss Core Version Check Remote Code Execution	CWE: 94  CVE: 2014-6261  BID: 71528	This strike exploits a remote code execution vulnerability in Zenoss Core. The flaw is due to a lack of authentication validation by the Zenoss Core Server during an update check. A remote unauthenticated attacker could exploit this vulnerability by enticing an authenticated user to perform an update check and spoofing a response, which could lead to arbitrary code execution on the target server.
Strike GNU Bash Trailing Characters After Function Definitions in Environment Variables Apace CGI Scripts	CWE: 78  CVE: 2014-6271  BID: 70103	This strike exploits a vulnerability in the GNU Bash which allows an attacker to execute arbitrary commands by providing them as trailing characters to an environment variable which holds a bash function. This strike exploits this vulnerability through Apache's mod_cgi module. If exploited the vulnerability results in remote code execution in the context of the user running the Apache process.
Strike Rejetto HTTP FileServer Remote Code Execution	CWE: 94  CVE: 2014-6287	This strike exploits a design weakness vulnerability in Rejetto HTTP FileServer. The vulnerability is due to improper validation of user supplied input. The findMacroMarker function in parserLib.pas allows an attacker to execute arbitrary programs via a null byte sequence in a search action. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the file server and might result in remote code execution.
Strike Microsoft Windows OLE Array Resize Memory Corruption	CWE: 119  CVE: 2014-6332  BID: 70952	This strike exploits a memory corruption vulnerability in Microsoft Windows OLE. VBScript has a function, redim preserve, which resizes an array while preserving the contents. If this is used with a very large value, it will trigger an error but not return the array to the original size, allowing read/write access outside the initial array bounds. A specially crafted HTML page can be used to trigger this vulnerability. Successful exploitation can result in execution of arbitrary code or abnormal termination of the browser.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer Data Prefix Memory Corruption	CWE: 399 CVE: 2014-6347 BID: 70347	This strike exploits a memory corruption vulnerability in Internet Explorer. The vulnerability is due to type-confusion when a DOMStringMap object is assigned to a text node property. An attacker could remotely execute arbitrary code by enticing a victim to view a malicious web page.
Strike Microsoft Internet Explorer CQuotes Use After Free Vulnerability	CWE: 399 CVE: 2014-6351 BID: 70323	This strike exploits a use-after-free vulnerability in Internet Explorer. The vulnerability occurs when an attempt is made to access a previously deleted CQuotes object. An attacker could remotely execute arbitrary code by enticing a victim to view a malicious web page.
Strike Internet Explorer base element Memory Corruption	CWE: 119 CVE: 2014-6366 BID: 71450	This strike exploits a Use-Afer-Free vulnerability in Internet Explorer. The vulnerability is due to an error triggered while processing dynamically added elements. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, causing arbitrary code to be executed on the victim system.
Strike GNU Bash Function Definitions in Environment Variables Apace CGI Scripts	CWE: 78 CVE: 2014-7169	This strike exploits a vulnerability in the GNU Bash also known as ShellShock which allows an attacker to execute arbitrary commands by providing them as functions to an environment variable. This strike exploits this vulnerability through Apache's mod_cgi module. If exploited the vulnerability results in remote code execution in the context of the user running the Apache process. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271.
Strike FreePBX Asterisk Recording Interface Cookie Unserialize Code Execution	CWE: 94 CVE: 2014-7235 BID: 70188	This strike exploits a code execution vulnerability in FreePBX Asterisk Recording Interface. The cookie ari_auth parameter receives a serialized PHP object which is not verified. An attacker can place a crafted serialized PHP object into the cookie ari_auth parameter to achieve code execution.
Strike ManageEngine Desktop Central DCPlugInServlet addPluginUser Policy Bypass	CWE: 264 CVE: 2014-7862 BID: 71849	This strike exploits a policy bypass vulnerability in ManageEngine Desktop Central. Authentication is not required to use the HTTP "action=addPlugInUser" parameter and value pair. An attacker may use this parameter to create and administrative account on the target system.
Strike ManageEngine Multiple Products Directory Traversal and File upload	CWE: 22 CVE: 2014-7866 BID: 71001	This strike exploits a directory traversal vulnerability in multiple ManageEngine products. The vulnerability is due to improper validation of the filename parameter. By exploiting this vulnerability, an attacker can upload files to arbitrary locations on the server and execute code.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Multiple ManageEngine Products APMBVHandler and DataComparisonServlet SQL Injection	CWE: 89 CVE: 2014-7868 BID: 71002	This strike exploits a SQL Injection vulnerability in multiple ManageEngine products. The vulnerability is due to insufficient sanitization of parameters in APMBVHandler and DataComparisonServlet servlets. By exploiting this vulnerability, an attacker can execute arbitrary SQL queries on the server.
Strike HP Point of Sale OPOS Driver oposstoneindicator Open Method Stack Buffer Overflow	CVE: 2014-7890 BID: 72969	This strike exploits a HP Point of Sale PC OPOS Driver vulnerability which is due to improper bound validation in the oposstoneindicator component. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike HP Point of Sale OPOS Driver POSKeyboard Buffer Overflow	CVE: 2014-7891 BID: 72969	This strike exploits a HP Point of Sale PC OPOS Driver vulnerability which is due to improper bound validation in the OPOSPOSKeyboard component. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike PHP Core Unserialize KeyName Use After Free	CVE: 2014-8142 BID: 71791	This strike exploits a use after free vulnerability in PHP. When PHP attempts to deserialize a specially crafted serializable object, a use after free may occur. Successful exploitation may result in arbitrary code executions with the privileges of the PHP application or abnormal program termination.
Strike Honeywell OPOS Suite Open Method HWOPSSCANNER Stack Buffer Overflow	CWE: 119 CVE: 2014-8269 BID: 71642	This strike exploits one of two buffer overflow vulnerabilities in the HWOPSSCANNER.ocx or HWOPSScale.ocx ActiveX controls within the HoneyWell OPOS Suite. The vulnerabilities are due to failure of the vulnerable methods to check the boundaries of user supplied input. By enticing a user to view a specially crafted web page, an attacker can execute code in the security context of the running process.
Strike Realtek SDK - Miniigd UPnP SOAP Remote Code Execution	CWE: 20 CVE: 2014-8361	This strike exploits a remote code execution on Realtek SDK Miniigd UPnP SOAP service. This vulnerability is due to improper handling of the parameter under xml tag when a client sends SOAP traffic to the server. A remote unauthenticated attacker can exploit this vulnerability by sending crafted http requests to the target server. Successful exploitation results in remote code execution.
Strike Advantech WebAccess SCADA webeye.ocx ActiveX ip_address Parameter Buffer Overflow	CWE: 119 CVE: 2014-8388 BID: 71193	This strike exploits a stack buffer overflow vulnerability in Advantech WebAccess SCADA software. The flaw is due to insufficient validation of input to the ip_addr parameter by the webeye.ocx ActiveX control. By enticing a user to visit a malicious web page, arbitrary code can be executed on the client system.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Visual Mining NetCharts Server HTTP Arbitrary File Upload	CWE: 434 CVE: 2014-8516 BID: 70895	This strike exploits an arbitrary file upload vulnerability in Visual Mining NetCharts Server. A specially crafted HTTP request can be sent to the server to upload arbitrary files. Further access to these files could lead to arbitrary code execution. This attack does require authentication, however there exist default, non-modifiable credentials in the software which can be used.
Strike NetBSD tnftp fetch.c fetch_url Command Execution	CWE: 77 CVE: 2014-8517 BID: 70792	This strike exploits a command execution vulnerability inside NetBSD tnftp client. The vulnerability is due to improper input validation of server supplied values and results in command execution in the context of the user running the client.
Strike Mozilla Firefox Proxy Prototype XrayWrapper Bypass Privilege Escalation	CWE: 94 CVE: 2014-8636 BID: 72041	This strike exploits a privilege escalation vulnerability in Mozilla Firefox. The vulnerability is due to the bypass of XrayWrappers, allowing web content to open a privileged window with the chrome property. An attacker could exploit this vulnerability by enticing a user to open a specially crafted webpage, resulting in execution of arbitrary code.
Strike WordPress Marketplace Remote Code Execution	CWE: 20 CVE: 2014-9013 BID: 73328 EXPLOITDB : 36490	This strike exploits a RCE vulnerability existent in the WordPress Marketplace plugin. This vulnerability is due to the lack of proper input sanitization while processing data from a POST request. An unauthenticated user could exploit this vulnerability by specially crafting a HTTP POST request with a call to wpmp_pp_ajax_call() method, which can lead to arbitrary code execution in the context of the vulnerable WP plugin.
Strike Schneider Electric ProClima ArrangeObjects Memory Corruption	CWE: 119 CVE: 2014-9188 BID: 71713	This strike exploits a memory corruption vulnerability in Schneider Electric ProClima MetaDraw ActiveX. The vulnerability is due to insufficient validation of a parameter from the ArrangeObjects method. By enticing a user to access a malicious web page, an attacker could execute code remotely in the context of the affected user.
Strike Advantech WebAccess AspVCOBJ ActiveX Multiple Buffer Overflow Vulnerabilities	CWE: 119 CVE: 2014-9208 BID: 76672	This strike exploits a vulnerability in Advantech WebAccess. The vulnerability is due to improper input validation of the argument given to InterfaceFilter, GetLastTagNbr, UpdateProjec or GetRecipeInfo methods in the AspVCOBJ ActiveX control. An attacker could exploit this vulnerability in order to remotely execute malicious code.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike SAP SQL Anywhere .NET Data Provider Scientific Notated Number Buffer Overflow	CWE: 119 CVE: 2014-9264 BID: 71627	This strike exploits a buffer overflow vulnerability in SAP SQL Anywhere .NET Data Provider. The vulnerable program fails to properly validate integers with multiple "e" or "E" scientific notation characters, and will copy the value into a fixed-length buffer. Successful exploitation may result in execution of arbitrary code with privileges of the .NET application or abnormal termination of the vulnerable application.
Strike Samsung SmartViewer CNC_Ctrl ActiveX Control Buffer Overflow	CWE: 119 CVE: 2014-9265 BID: 71486	This strike exploits a stack buffer overflow vulnerability in Samsung SmartViewer CNC_Ctrl ActiveX. The flaw is due to insufficient validation of input to the BackupToAvi method by the CNC_Ctrl ActiveX control. By enticing a user to visit a malicious web page, arbitrary code can be executed on the client system.
Strike Microsoft Internet Explorer CAutoRange ScrollIntoView Memory Corruption	CWE: 399 CVE: 2015-0017 BID: 72402	This strike exploits a Memory Corruption vulnerability in Internet Explorer. The vulnerability is due to the manner in which Internet Explorer processes selections and scrolling. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.
Strike Microsoft Internet Explorer CShadow Direction Integer Overflow	CWE: 399 CVE: 2015-0036 BID: 72446	This strike exploits an Integer Overflow vulnerability in Internet Explorer. The vulnerability is due to the failure of the CShadow::put_Direction function to sanitize user-supplied input. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.
Strike Microsoft Internet Explorer X509EnrollmentWeb ClassFactory Type Confusion Memory Corruption	CWE: 399 CVE: 2015-0046 BID: 72416	This strike exploits a Memory Corruption Vulnerability in the Microsoft Internet Explorer X509EnrollmentWebClassFactory ActiveX Control. An attacker can entice a victim to visit a specially crafted web page using the vulnerable control. Successful exploitation can result in execution of arbitrary code or abnormal termination of Internet Explorer.
Strike Microsoft Internet Explorer DOM Style Postion Memory Corruption	CWE: 399 CVE: 2015-0053 BID: 72421	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer. An HTML DOM object with specially crafted style values can be used to trigger memory corruption. Successful exploitation may result in execution of arbitrary code or abnormal termination of Internet Explorer.
Strike Microsoft Internet Explorer BuildAnimation Memory Corruption	CWE: 399 CVE: 2015-0099 BID: 72925	This strike exploits a Memory Corruption vulnerability in Internet Explorer. The vulnerability occurs when certain CSS directives are used during key frame creation. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer CTreeNode Use-After-Free	CWE: 119 CVE: 2015-0100 BID: 72926	This strike exploits a Use-After-Free vulnerability in Internet Explorer. The vulnerability is due to an error while handling CTreeNode objects. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.
Strike PHP Core Unserialize Numeric KeyName Use After Free	CVE: 2015-0231 BID: 72539	This strike exploits a use after free vulnerability in PHP. When PHP attempts to deserialize a specially crafted serializable object, a use after free may occur. Successful exploitation may result in arbitrary code executions with the privileges of the PHP application or abnormal program termination.
Strike GNU C Library (glibc) gethostname Function Heap Buffer Overflow - Wordpress XML-RPC	CWE: 119 CVE: 2015-0235 BID: 72325	This strike exploits a heap buffer overflow within glibc, used by Wordpress XML-RPC. The vulnerability is due to a failure to validate user input within the gethostbyname function. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted XML-RPC request, resulting in arbitrary code execution on the targeted system.
Strike PHP DateTime Object Unserialize Use After Free	CVE: 2015-0273 BID: 72701 EXPLOITDB : 36158	This strike exploits a vulnerability PHP which is triggered when trying to unserialize a serialized DateTime object. The vulnerability can be exploited through user supplied parameters which are then passed to the vulnerable function. If exploited the vulnerability can result in remote code execution under the context of the service running the PHP server.
Strike Oracle Data Quality LoaderWizard ActiveX SetEntities Type Confusion	CVE: 2015-0444 BID: 75803	This strike exploits a type confusion vulnerability in Oracle Data Quality. The ActiveX control TSS12.LoaderWizard.lwctrl has a function SetEntities, which expects a VARIANT type parameter. If the function receives an unexpected type, it leads to an arbitrary pointer dereference. Successful exploitation may result in execution of arbitrary code or abnormal browser termination.
Strike Cisco Data Center Network Manager FileServlet Class Information Disclosure	CWE: 22 CVE: 2015-0666 BID: 73479	This strike exploits a Cisco Data Center Network Manager directory traversal vulnerability which is due to improper parameter validation in the FileServlet class doGet method. By exploiting this vulnerability sensitive information could be obtained, which could be used in a remote code execution attack.
Strike Novell Zenworks Configuration Management remote code execution	CWE: 22 CVE: 2015-0779 BID: 73949	This strike exploits a directory traversal vulnerability in Novell ZenWorks Configuration Management. The vulnerability is due to improper handling of the uid parameter in UploadServlet. By exploiting this vulnerability, an unauthenticated attacker can upload files in arbitrary locations on the server and execute them. NOTE: By default the vulnerable services are accessed via SSL connection (port 443)

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Novell Zenworks Configuration Management GetStoredResult SQL Injection	BID: 74284 CWE: 89 CVE: 2015-0780	This strike exploits a SQL injection vulnerability in Novell Zenworks Configuration Management. The vulnerability is due to improper validation of user supplied input in the GetStoredResult action. By exploiting this vulnerability, an unauthenticated attacker can execute arbitrary SQL queries on the server.
Strike Novell Zenworks Configuration Management Rtrlet Directory Traversal	CWE: 22 CVE: 2015-0781 BID: 74291	This strike exploits a directory traversal vulnerability in Novell Zenworks Configuration Management. The vulnerability is due to improper validation of user supplied data in the Rtrlet class when uploading files to the server. By exploiting this vulnerability, an unauthenticated attacker can upload files to arbitrary locations on the server and execute them.
Strike Novell Zenworks Configuration Management scheduleQuery SQL Injection	CWE: 89 CVE: 2015-0782 BID: 72808	This strike exploits an SQL injection vulnerability in Novell Zenworks Configuration Management. The vulnerability is due to improper sanitization of user supplied input in the scheduleQuery action. An authenticated attacker can exploit this vulnerability in order to execute arbitrary SQL queries on the target system. NOTE: By default the vulnerable services are accessed via SSL connection (port 443).
Strike Novell ZENworks Configuration Management Directory Traversal	CWE: 200 CVE: 2015-0785 BID: 74288	This strike exploits a directory traversal vulnerability inside Novell ZENworks Configuration Management. The vulnerability is due to improper parameter validation in the DirectoryViewer run method. An attacker could exploit this vulnerability in order to gain unauthorized access to information or services. NOTE: By default the vulnerable services are accessed via SSL connection (port 443).
Strike NetIQ Solutions Safeshellexecute buffer overflow	CWE: 119 CVE: 2015-0795 BID: 75903	This strike exploits a buffer overflow vulnerability in NETIQExecObject.NetIQExec ActiveX Control. The vulnerability is due to improper validation of parameters in the SafeShellExecute method. By enticing a user to access a specially crafted web page, an attacker can execute arbitrary code on the target's system.
Strike Sefrengo CMS idclient and idcat SQL Injection	CWE: 89 CVE: 2015-0919 BID: 71885	This strike exploits a SQL injection in Sefrengo CMS. The vulnerability is due to improper sanitization of user supplied input in idcat and idclient parameters in /backend/main.php. By exploiting this vulnerability, an authenticated attacker can execute arbitrary SQL queries on the server.
Strike Schneider Electric DS-NVs RVControl Buffer Overflow	CWE: 119 CVE: 2015-0982 BID: 73096	This strike exploits a Schneider Electric Pelco DS-NV Software package vulnerability which is due to improper bound validation in the SetText method. An attacker could exploit this vulnerability in order to remotely execute malicious code.

Name	References	Description
Strike D-Link DnsProxy Cross Site Scripting (XSS)	CWE: 79 CVE: 2015-1028 EXPLOITDB : 35750 BID: 72725	This strike exploits a stored cross-site scripting (XSS) vulnerability in D-Link DSL-2730B Modem. The vulnerability is due to improper validation of HTTP request domainname parameter. By exploiting this vulnerability an attacker could execute arbitrary scripts on the target machine.
Strike Safari Cross-Domain Vulnerability	CWE: 20 CVE: 2015-1126 BID: 73977	This strike exploits a Safari cross-domain vulnerability which is due to improper FTP URL sanitization. By exploiting this vulnerability an attacker could gain unauthorized access to information or services.
Strike Privilege Escalation Vulnerability Inside Apple CUPS	CWE: 254 CVE: 2015-1158 BID: 75098	This strike exploits an elevation-of-privilege vulnerability inside Apple CUPS. The vulnerability is due to improper processing of certain requests in the add_job method. An attacker could exploit this vulnerability in order to gain root privileges and execute malicious code on the target machine.
Strike Cross-Site Scripting (XSS) Vulnerability Inside Apple CUPS Web Interface	CWE: 79 CVE: 2015-1159 BID: 75106	This strike exploits a cross-site scripting vulnerability inside Apple CUPS Web interface. The vulnerability is due to improper input validation in the cgi_puts method. By exploiting this vulnerability an attacker could execute malicious scripts on the target machine.
Strike ElasticSearch Search Groovy Sandbox Bypass Vulnerability	CWE: 284 CVE: 2015-1427 BID: 72585	This strike exploits a sandbox-bypass vulnerability in ElasticSearch. The vulnerability is due to a failure to sanitize user supplied input, java code to be executed via reflection. Exploiting this vulnerability could allow remote, unauthenticated attackers to execute arbitrary code on the target server.
Strike Sefrengo CMS Login Cookie SQL Injection	CWE: 89 CVE: 2015-1428 BID: 72452	This strike exploits a SQL injection vulnerability in Sefrengo CMS. The vulnerability is due to improper sanitization of the cookie in HTTP requests. The vulnerable file is /backend/main.php. By exploiting this vulnerability, an unauthenticated attacker can execute arbitrary SQL queries on the server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Sefrengo CMS value_id SQL Injection	CWE: 89 CVE: 2015-1428 BID: 72452	This strike exploits a SQL injection in Sefrengo CMS. The vulnerability is due to improper sanitization of user supplied input in /backend/main.php. The vulnerable parameter is value_id. By exploiting this vulnerability, an authenticated attacker can execute arbitrary SQL queries on the server.
Strike ManageEngine ServiceDesk Plus Privilege Bypass Information Disclosure	CWE: 200 CVE: 2015-1480 BID: 72302	This strike exploits a directory traversal vulnerability in ServiceDesk. A non-administrator user can access certain directories which should be restricted to administrators due to insufficient validation. Successful exploitation can result in disclosure of information.
Strike Symantec Endpoint Protection ConsoleServlet Policy Bypass Vulnerability	CWE: 287 CVE: 2015-1486 BID: 76074	This strike exploits a policy bypass vulnerability in Symantec Endpoint Protection. The vulnerability is due to improperly sending a valid session token to unauthenticated users that request a password reset for the admin account. An attacker could exploit this vulnerability in order get access on the target machine. NOTE: By default the vulnerable services are accessed via SSL connection (port 8443).
Strike Multiple Vulnerabilities in Samsung Security Manager ActiveMQ	CWE: 264 CVE: 2015-1499 BID: 72598	This strike exploits multiple code execution vulnerabilities inside Samsung Security Manager ActiveMQ. These vulnerabilities are due to permitting unauthenticated access to ActiveMQ Fileserver. An attacker could exploit this vulnerability in order to gain unauthorized access and run malicious code on the target machine.
Strike SolarWinds Server and Application Monitor loadExtensionFactor y Stack Buffer Overflow	CWE: 119 CVE: 2015-1500 BID: 72600	This strike exploits a buffer overflow vulnerability in SolarWinds Orion Server and Application Monitor that is due to lack of boundary validation. Exploitation of this vulnerability results in a remote code execution attack.
Strike IceWarp Mail Server under 11.1.1 - Directory Traversal	CWE: 22 CVE: 2015-1503 EXPLOITDB : 44587	This vulnerability in IceWarp Mail Server under version 11.1.1 allows attackers read access to arbitrary file content by directory traversal due to insufficient validation of http parameter "script".
Strike Dell ScriptLogic Asset Manager GetClientPackage SQL Injection	CWE: 89 CVE: 2015-1605 BID: 72697	This strike exploits a SQL injection vulnerability in Dell ScriptLogic Asset Manager. The vulnerability is due to improper sanitization of parameters in HTTP requests. By exploiting this vulnerability, an unauthenticated attacker can inject and execute SQL queries, leading to disclosure or manipulation of data on the server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer CGeneratedContent Memory Corruption	BID: 72927 CWE: 399 CVE: 2015-1622	This strike exploits a Microsoft Internet Explorer vulnerability which is due to an out-of-bounds write while style processing HTML elements. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike Microsoft HTTP.sys Remote Code Execution Vulnerability	CWE: 94 CVE: 2015-1635 BID: 74013	This strike exploits an integer overflow vulnerability in Microsoft HTTP.sys. The vulnerability is caused by an integer overflow which may occur when processing specially crafted HTTP requests. Successful exploitation could lead to remote code execution under the System account or to a denial of service.
Strike Internet Explorer Tree TextData Use After Free	CWE: 399 CVE: 2015-1665 BID: 74000	This strike exploits a use after free vulnerability in Microsoft Internet Explorer. The vulnerability is caused by incorrect management of TextData objects when processing HTML and Javascript code. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to view a specially crafted HTML file, possibly resulting in remote code execution in the security context of the target user.
Strike Internet Explorer CVE-2015-1667 Use After Free	CWE: 399 CVE: 2015-1667 BID: 74003	This strike exploits a use after free vulnerability in Microsoft Internet Explorer. The vulnerability is caused by incorrect management of CQuotes objects when processing HTML and Javascript code. A remote unauthenticated attacker could exploit this vulnerability by enticing a user to view a specially crafted HTML file, possibly resulting in remote code execution in the security context of the target user.
Strike Microsoft Internet Explorer SVG Marker Object Use-After-Free	CWE: 399 CVE: 2015-1668 BID: 74004	This strike exploits a Use-After-Free vulnerability in Internet Explorer. The vulnerability is due to an error while handling CGeneratedTreeNode objects. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.
Strike Information Disclosure Vulnerability in Microsoft Windows VBScript	CWE: 200 CVE: 2015-1684 BID: 74522	This strike exploits a regular expression information disclosure vulnerability inside Microsoft Windows VBScript . This vulnerability is due to improper processing of regular expressions. An attacker could exploit this vulnerability in order to gain unauthorized access to information or services.
Strike Information Disclosure Vulnerability in Microsoft Internet Explorer	CWE: 200 CVE: 2015-1692 BID: 74517	This strike exploits an information disclosure vulnerability inside Microsoft Internet Explorer. The vulnerability is due to improper access to system clipboard through copy, cut and paste events. An attacker could exploit this vulnerability in order to gain unauthorized access to information or services.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer CParamElement Use-After-Free	CWE: 119 CVE: 2015-1705 BID: 74509	This strike exploits a Use-After-Free vulnerability in Internet Explorer. The vulnerability is due to an error while handling CParamElement objects. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.
Strike Internet Explorer memory corruption	CWE: 399 CVE: 2015-1744 BID: 74984	This strike exploits a use after free vulnerability in Internet Explorer. The vulnerability is due to the way first-line and first-letter element styling are handled in HTML code. By enticing a user to access a specially crafted web page, a remote unauthenticated attacker can execute arbitrary code in the security context of the target user.
Strike Memory Corruption Vulnerability Inside Microsoft Internet Explorer	CWE: 399 CVE: 2015-1745 BID: 74985	This strike exploits a memory corruption vulnerability inside Microsoft Internet Explorer . The vulnerability is due to an error that occurs when CAttrValue objects are created with uninitialized data. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike Microsoft Internet Explorer ArrayBuffer Write What Where	CWE: 399 CVE: 2015-1747 BID: 74986	This strike exploits a write-what-where condition in Microsoft Internet Explorer version 11. The vulnerability is caused by improper invalidation of an ArrayBuffer object. A remote, unauthenticated attacker could exploit this vulnerability by enticing a user to access a crafted HTML page. Successful exploitation would result in code execution in the context of the user accessing the web page.
Strike Microsoft Internet Explorer execCommand AutoDetect Crafted Url Memory Corruption	CWE: 399 CVE: 2015-1752 BID: 74989	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer. An HTML DOM execCommand AutoDetect can be caused to read out-of-bounds by a specially crafted URL string. An attacker can entice a target to visit a specially crafted webpage to trigger the exploit. Successful exploitation can result in execution of arbitrary code, information disclosure, or abnormal termination of Internet Explorer.
Strike Apache ActiveMQ File Upload Directory Traversal Vulnerability	CWE: 22 CVE: 2015-1830 BID: 76452	This strike exploits a directory traversal vulnerability in Apache ActiveMQ. The vulnerability is due to improper validation of destination HTTP header. Using a crafted URI, an attacker could upload a malicious executable to be executed on the target server.

Name	References	Description
Strike D-Link HNAP SOAPAction Header Command Execution	CWE: 77 CVE: 2015-2051 BID: 74870 EXPLOITDB : 37171	This strike exploits a vulnerability in D-Link DIR-645 Wired/Wireless Router. Specially crafted HTTP messages can be sent to a vulnerable device to achieve arbitrary code execution via HNAP interface.
Strike Agilent Technologies Feature Extraction Insert Method Out-Of-Bounds Indexing	CWE: 119 CVE: 2015-2092 BID: 72840	This strike exploits an out-of-bounds indexing vulnerability in Agilent Technologies Feature Extraction. The vulnerability is caused by improper validation of a parameter to the Insert method. A remote, unauthenticated attacker could exploit this vulnerability by crafting a malicious page and enticing a user to access it. Successful exploitation could lead to code execution in the security context of the application.
Strike WebGate WESPPPlayback Stack Buffer Overflow	CWE: 119 CVE: 2015-2094 BID: 72841	This strike exploits a WebGate WESPPPlaybackCtrl control vulnerability that appears in multiple products. This vulnerability is due to improper bound validation in the PlaySiteAllChannel, StopSiteAllChannel, PrintSiteImage and SaveSiteImage methods. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike WebGate Multiple Products WESPMonitor Stack Buffer Overflow	CWE: 119 CVE: 2015-2097 BID: 72835	This strike exploits a stack buffer overflow vulnerability in multiple WebGate products in the WESPMonitorCtrl ActiveX control. The vulnerability is due to improper validation of a parameter in LoadImage and LoadImageEx methods. By enticing a user to access a specially crafted web page, an attacker could execute arbitrary code.
Strike WebGate eDVR Manager WESPPPlayback SiteName Stack Buffer Overflow	CVE: 2015-2098 BID: 72838	This strike exploits a WebGate eDVR Manager WESPPPlaybackCtrl ActiveX buffer overflow vulnerability. This vulnerability is due to improper bound validation for the SiteName property. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike WebGate WESPSDK WESPDiscovery Stack Buffer Overflow	CVE: 2015-2100 BID: 72843	This strike exploits a buffer overflow vulnerability in WebGate WESPSDK WESPDiscovery ActiveX. The vulnerability is due to improper validation of a parameter in TCPDiscovery and TCPDiscovery2 methods. By enticing a user to access a specially crafted web page, an attacker could execute arbitrary code.
Strike HP SiteScope Log Analyzer Information Disclosure	CVE: 2015-2120 BID: 74801	This strike exploits an information disclosure vulnerability in HP SiteScope LogAnalyzer versions 11.1x before 11.13, 11.2x before 11.24.391, and 11.3x before 11.30.521. The vulnerability is caused by improper validation of a user-supplied file path, allowing a user to, among others, load user passwords from the users.config file. An authenticated attacker could exploit this by choosing a filename which would then disclose user passwords, possibly leading to privilege escalation to the administrator role.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike PHPMoAdmin Unauthorized Remote Code Execution	CWE: 77 CVE: 2015-2208	This strike exploits an arbitrary code execution vulnerability in phpMoAdmin. The vulnerability is due to unsanitized evaluation of user-supplied input via http. An attacker could exploit this vulnerability to remotely execute arbitrary code on the target system.
Strike SolarWinds Firewall Security Manager userlogin.jsp Policy Bypass	CWE: 264 CVE: 2015-2284	This strike exploits a policy bypass vulnerability in SolarWindws Firewall Security Manager. The vulnerability is due to improper handling of parameters in userlogin.jsp. By exploiting this vulnerability, an attacker can add, modify, remove or impersonate users without authentication.
Strike Electric Sheep Fencing pfSense Directory Traversal	CWE: 352 CVE: 2015-2295 BID: 73344	This strike exploits an Electric Sheep Fencing pfSense directory traversal vulnerability which is due to improper parameter validation. By exploiting this vulnerability an attacker could delete private information which could lead to a denial of service attack.
Strike Microsoft Internet Explorer Memory Corruption Vulnerability	CWE: 119 CVE: 2015-2391	This strike exploits a memory corruption vulnerability inside Microsoft Internet Explorer. The vulnerability is due to an error that occurs when trying to free an internal structure 2 times. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike Internet Explorer Javascriptexecption sOperator memory corruption	CWE: 119 CVE: 2015-2443 BID: 76195	This strike exploits a type confusion vulnerability in Microsoft Internet Explorer. The vulnerability is due to improper handling of a parameter in the accessor function for the stack trace property descriptor. An attacker can entice a target to visit an specially crafted HTML page in order to trigger the vulnerability. Successful exploitation can result in execution of arbitrary code or abnormal termination of Internet Explorer.
Strike Microsoft Internet Explorer CSS Style Behavior Property Use After Free	CWE: 119 CVE: 2015-2444 BID: 76194	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically the vulnerability exists when a CSS style assigned to a child element of an HTML element is overwritten through reloading the window. If the object is deleted a reference to it remains and any further attempts to access the freed object result in a use-after-free condition.
Strike CInput Memory Corruption Vulnerability In Microsoft Internet Explorer	CWE: 119 CVE: 2015-2446 BID: 76193	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer. The vulnerability is due to a user-after-free condition that can be triggered when dealing with CInput objects. An attacker could exploit this vulnerability in order to remotely execute malicious code.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Type Confusion Vulnerability In Microsoft Internet Explorer	CWE: 119 CVE: 2015-2448 BID: 76191	This strike exploits a type confusion vulnerability in Microsoft Internet Explorer. The vulnerability is due to an error that occurs when handling an Array's call function, which does not verify that the first parameter is an object. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike Microsoft Internet Explorer WMPlayer Use-After-Free	CWE: 119 CVE: 2015-2487 BID: 76574	This strike exploits a Use-After-Free vulnerability in Internet Explorer. The vulnerability occurs when Internet Explorer interacts with Windows Media Player in the handling certain HTML objects. An attacker could exploit this vulnerability by enticing a user to view a malicious web page, executing arbitrary code on the victim machine.
Strike Microsoft Internet Explorer Memory Corruption Vulnerability Through Table Element	BID: 76580 CWE: 119 CVE: 2015-2499	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer. The vulnerability is due to a out-of-bounds memory access condition that can be triggered when dealing with table elements constructed in a certain way. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike Microsoft Windows Shell Toolbar Object Use After Free	CWE: 416 CVE: 2015-2515 BID: 76981	This strike exploits a use after free vulnerability in Microsoft Windows Shell. The vulnerability is triggered by accessing a CQuickLinksobject after its deletion. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike Microsoft Windows Tablet Input Band Object Use After Free	CVE: 2015-2548 BID: 76989	This strike exploits a use after free vulnerability in Microsoft Tablet Input Band. The vulnerability is triggered by accessing a CDeskBand object after its deletion. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike ManageEngine Desktop Central Unauthorized Administrative Password Reset	BID: 73380 CWE: 264 CVE: 2015-2560	This strike exploits an access control vulnerability in ManageEngine Desktop Central. The vulnerability is due to lack of authentication checks on DCOperationsServlet. By exploiting this vulnerability, an unauthenticated attacker can modify password for privileged accounts and gain administrative access in the application.
Strike Oracle Endeca Information Discovery Integrator ETL Server Directory Traversal Vulnerability Through CopyFile	CVE: 2015-2604 BID: 75757	This strike exploits a directory traversal vulnerability in Oracle Endeca Information Discovery Integrator ETL Server. The vulnerability is due to improper validation of parameters when handling CopyFile operation in SOAP requests. An attacker could exploit this vulnerability in order to gain unauthorized access to information or services.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle Endeca Information Discovery Integrator ETL Server Directory Traversal Vulnerability Through MoveFile	CVE: 2015-2605 BID: 75756	This strike exploits a directory traversal vulnerability in Oracle Endeca Information Discovery Integrator ETL Server. The vulnerability is due to improper validation of parameters when handling MoveFile operation in SOAP requests. An attacker could exploit this vulnerability in order to gain unauthorized access to information or services.
Strike Oracle Endeca Information Discovery CloverServerWSImpl directory traversal	CVE: 2015-2606 BID: 75758	This strike exploits a directory traversal vulnerability in Oracle Endeca Information Discovery Integrator ETL Server. The vulnerability is due to insufficient validation of user supplied input in RenameFile SOAP requests. By exploiting this vulnerability, an authenticated attacker can move arbitrary files on the vulnerable server in order to disclose sensitive information.
Strike Wordpress Simple Ads Manager SQL Injection	CWE: 89 CVE: 2015-2824 BID: 73698	This strike exploits a SQL injection vulnerability in WordPress Simple Ads Manager. The vulnerability is due to failure to sanitize user-controlled input in sam-ajax.php and sam-ajax-admin.php. By exploiting this vulnerability, an unauthenticated attacker can execute arbitrary SQL queries on the server.
Strike Wordpress Simple Ads Manager Arbitrary File Upload	CVE: 2015-2825 BID: 73924	This strike exploits a directory traversal vulnerability in Wordpress Simple Ads Manager. The vulnerability is due to lack of sanitization of the path parameter in sam-ajax-admin.php. By exploiting this vulnerability, an unauthenticated attacker can upload arbitrary files on the server and execute them.
Strike Wordpress Simple Ads Manager Information Disclosure	CWE: 200 CVE: 2015-2826 BID: 73924	This strike exploits an information disclosure vulnerability in Wordpress Simple Ads Manager. The vulnerability is due to improper handling of the action parameter in sam-ajax-admin.php. The vulnerability can be exploited through sam-ajax-admin.php and allows remote unauthenticated information disclosure from the database available in the application.
Strike TP-Link Archer Devices Directory Traversal	CWE: 22 CVE: 2015-3035	This strike exploits a directory traversal vulnerability in TP-Link Archer Devices. This vulnerability is due to insufficient input validation. A remote, unauthenticated attacker could exploit this vulnerability to read sensitive information from arbitrary files located on the file system of the target server.
Strike cURL and libcurl sanitize_cookie_path remote code execution	CWE: 119 CVE: 2015-3145 BID: 74303	This strike exploits a remote code execution vulnerability in cURL and libcurl. The vulnerability is due to improper validation of the Set-Cookie header. An unauthenticated attacker can exploit this vulnerability in order to execute arbitrary code on the target system. Unsuccessful exploitation may lead to a denial of service condition on the target system.

Name	References	Description
Strike WordPress Comment Cross Site Scripting (XSS)	CWE: 79 CVE: 2015-3440 BID: 74334	This strike exploits a cross-site scripting vulnerability in Wordpress. The vulnerability is due to improper validation of HTTP request comment parameter. By exploiting this vulnerability an attacker could execute arbitrary scripts on the target machine.
Strike Magento Forwarded Authentication Bypass	CWE: 287 CVE: 2015-3457 BID: 74420	This strike exploits an authentication bypass vulnerability in Magento. The vulnerability is due to improper handling of unauthenticated requested actions with the forwarded parameter set. By exploiting this vulnerability, an unauthenticated attacker can perform administrative actions without any prior authentication.
Strike Bonita BPM themeResource directory traversal arbitrary file disclosure	CWE: 22 CVE: 2015-3897	This strike exploits a directory traversal vulnerability in Bonita BPM. The vulnerability is due to lack of validation of user supplied parameters in themeResource web page An unauthenticated attacker can exploit this vulnerability in order to reveal the contents of files from any location on the vulnerable server.
Strike PHP tar Zero Length File Name Integer Overflow	CWE: 189 CVE: 2015-4021 BID: 74700	This strike exploits an integer overflow vulnerability in PHP. When PHP processes a tar file, it determines the length of the filename by the displacement of the first null byte. A later calculation subtracts 1 from this length. If the calculated length was zero, the calculation results in an unsigned integer overflow, allowing access to a large portion of the heap. Successful exploitation may result in execution of arbitrary code with privileges of the service running PHP or abnormal termination of the service.
Strike Visual Mining NetCharts Server saveFile.jsp Directory Traversal	CWE: 22 CVE: 2015-4031 BID: 74792	This strike exploits a directory traversal vulnerability in Visual Mining NetCharts Server versions 7.0.1 and prior. The vulnerability is caused by improper sanitization of the filename parameter in a request to saveFile.jsp. An unauthenticated remote attacker could exploit this vulnerability by sending a crafted HTTP request to the target application, leading to file upload and remote code execution under the credentials of the process running the web server (by default, System).
Strike Visual Mining Netcharts Server projectContents.jsp directory traversal	CWE: 264 CVE: 2015-4032 BID: 74788	This strike exploits a directory traversal vulnerability in Visual Mining NetCharts Server. The vulnerability is due to improper validation of the project parameter in projectContents.jsp when renaming project files. By exploiting this vulnerability, an unauthenticated attacker can rename arbitrary files on the server, which can result in a denial of service condition.

Name	References	Description
Strike Adobe Flash Nellymoser audio Codec Heap Overflow	CWE: 119 CVE: 2015-4432 GOOGLE: 425 BID: 75592	This strike exploits a remote code execution vulnerability in Adobe Flash Player. The vulnerability is due to a heap overflow when loading FLV file with Nellymoser audio codec. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in execution of arbitrary code or abnormal termination of the flash process.
Strike OpenEMR Authentication Bypass Vulnerability	CWE: 287 CVE: 2015-4453 BID: 75299	This strike exploits an authentication bypass vulnerability in OpenEMR. The vulnerability is due to improper HTTP parameter extraction. An attacker could exploit this vulnerability in order to obtain unauthorized access.
Strike Mozilla Firefox Pdf.js Same Origin Policy Bypass	CVE: 2015-4495 CWE: 346	This strike exploits the Same-Origin Policy Bypass Vulnerability against Mozilla Firefox. The Vulnerability is due to a design flaw in the built-in PDF Viewer of the application. A remote unauthenticated attacker can exploit this vulnerability by enticing a user to visit a specially crafted webpage. Successful Exploitation would result in the disclosure of sensitive information.
Strike Panasonic Security Ipropsapi ActiveX FilePassword Buffer Overflow	BID: 75409 CWE: 119 CVE: 2015-4647	This strike exploits a buffer overflow vulnerability in Panasonic Security API Ipropsapi ActiveX Control. The vulnerability is due to improper validation of the FilePassword property. By enticing a user to access a specially crafted web page, an attacker can execute arbitrary code.
Strike Panasonic Security Ipropsapi ActiveX MulticastAddr Buffer Overflow	CWE: 20 CVE: 2015-4648 BID: 75405	This strike exploits a buffer overflow vulnerability in Panasonic Security API Ipropsapi ActiveX Control. The vulnerability is due to improper validation of the MulticastAddr property. By enticing a user to access a specially crafted web page, an attacker can execute arbitrary code.
Strike Oracle Data Quality SetBasicPreviewData type confusion	CVE: 2015-4759 BID: 75806	This strike exploits a code execution vulnerability in Oracle Data Quality TSS12.LoaderWizard.Iwctrl ActiveX. The vulnerability is due to improper handling of native Javascript objects by the SetBasicPreviewData method. An unauthenticated attacker can exploit this vulnerability by enticing a user to view a specially crafted web page. Successful exploitation can lead to remote code execution.

Name	References	Description
Strike Endian Firewall Proxy Reset Pasword Command Execution	CWE: 77 CVE: 2015-5082 EXPLOITDB : 38096 BID: 76865	This strike exploits a input validation error present in Endian Firewall. Vulnerability can be exploited by crafting a special HTTP request to the target. Successful exploitation would result in arbitrary command execution in the security context of Apache httpd server.
Strike Adobe Flash ActionScript 3 ByteArray Use After Free	CWE: 119 CVE: 2015-5119 BID: 75568	This strike exploits a use after free vulnerability in Adobe Flash. If a ByteArray object contains a class instance which resizes the ByteArray, new memory will be allocated for the ByteArray, but a Vector object may be written in the address of the old ByteArray, a use after free condition. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in execution of arbitrary code or abnormal termination of the flash process.
Strike Apache Software Foundation Subversion Integer Overflow Vulnerability	CWE: 119 CVE: 2015-5343	This strike exploits an integer overflow vulnerability in Apache Software Foundation Subversion. The vulnerability is due to improper validation of HTTP Content-Length header before allocating a heap buffer based on this length. An attacker could exploit this vulnerability in order to remotely execute arbitrary code or cause a denial of service condition on the target machine.
Strike Adobe Flash MP3 ID3 Integer Overflow	CWE: 189 CVE: 2015-5560 BID: 76289 EXPLOITDB : 37882	This strike exploits an integer overflow vulnerability in Adobe Flash Player. The vulnerability is due to a failure when handling malformed MP3 files. An attacker could exploit this vulnerability by enticing a user to open a malicious file with the vulnerable software, potentially executing arbitrary code.
Strike Adobe Flash Player Wild write in Color Conversion Memory Corruption	CWE: 119 CVE: 2015-5575 GOOGLE: 452 BID: 76799	This strike exploits a remote code execution vulnerability in Adobe Flash Player. The vulnerability is due to a wild write at 0x453b0cf0 in color conversion. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in execution of arbitrary code or abnormal termination of the flash process.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Adobe Flash Audio Handling Read Out Of Bound	CWE: 119 CVE: 2015-5577 BID: 76799 GOOGLE: 449	This strike exploits a remote code execution vulnerability in Adobe Flash Player. The vulnerability is due to an out-of-bounds read when Adobe flash loads the MP4 file using Sound.extract() or a similar API. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in abnormal termination of the flash process.
Strike OpenDocMan Cross-Site Scripting (XSS)	CWE: 79 CVE: 2015-5625 BID: 76627	This strike exploits a cross-site scripting vulnerability in OpenDocMan Web interface. The vulnerability is due to improper validation of HTTP request parameters. By exploiting this vulnerability an attacker could execute arbitrary scripts on the target machine.
Strike WordPress KSES Bypass Cross Site Scripting (XSS)	CWE: 79 CVE: 2015-5714 BID: 76745	This strike exploits a cross-site scripting vulnerability in Wordpress. The vulnerability is due to improper validation of content in blog when using short code. By exploiting this vulnerability an attacker could execute arbitrary scripts on the target machine.
Strike Websense Content Gateway HTTP Parameter cmd_param Buffer Overflow	CWE: 119 CVE: 2015-5718 BID: 75160	This strike exploits a buffer overflow vulnerability inside Websense Content Manager administrative interface. The vulnerability is due to improper validation of cmd_param HTTP parameter. An attacker could exploit this vulnerability in order to remotely execute malicious code on the target machine.
Strike Typo3 CMS Cross Site Scripting (XSS)	CWE: 79 CVE: 2015-5956 BID: 76692	This strike exploits a cross-site scripting vulnerability in Typo3 CMS. The vulnerability is due to improper validation of HTTP request returnUrl and redirect_url HTTP parameters. By exploiting this vulnerability an attacker could execute arbitrary scripts on the target machine.
Strike Microsoft Internet Explorer CWindow Object Use After Free	CVE: 2015-6042 BID: 76984	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically a use after free vulnerability occurs when an iframe element is encountered pointing to code in which a CWindow object is created. If the children of this object are deleted upon invoking an event listener, memory corruption can occur leading a use after free condition. It is possible that an attacker can control this, potentially leading to remote code execution, or a denial of service in the Internet Explorer application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer COM object Use After Free	CWE: 119 CVE: 2015-6049 BID: 76986	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically the vulnerability is found in iframe.dll, and is due to the deletion of a CISFBand object. When the page is reloaded and an attempt to access that deleted object is made, a use-after-free condition occurs, which can lead to memory corruption.
Strike Microsoft Internet Explorer ArrayBuffer Information Disclosure	CWE: 200 CVE: 2015-6053 BID: 76995	This strike exploits an information disclosure vulnerability in Microsoft Internet Explorer. The vulnerability is due to the way the ArrayBuffer.slice method handles transfer of information between different browser windows. An attacker could exploit this vulnerability in order to access private information.
Strike Microsoft Internet Explorer Onresize Use After Free	CWE: 119 CVE: 2015-6071	This strike identifies a user after free vulnerability in Internet Explorer. Specifically, if a form element contains an input element and the value of that input element is changed an onresize event of the form id1ect is triggered. Next the form id1ect's event handler tries to reference an element that does not exist causing memory corruption to occur.
Strike Microsoft Internet Explorer CTableRow Object Memory Corruption	CWE: 119 CVE: 2015-6083 BID: 78481	This strike identifies a vulnerability in Microsoft Internet Explorer. This vulnerability is due to the way Internet Explorer handles certain table element objects. Specifically when a CTableRow object is allocated and insertRow is called on that object with an uninitialized pointer as a parameter that belongs to the allocated object memory corruption can occur.
Strike Microsoft Internet Explorer DOM SVG TextBox Object Type Confusion Memory Corruption	CWE: 119 CVE: 2015-6085 BID: 77456	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer. A specially crafted webpage with certain manipulations of DOM SVG TextBox objects with nested HTML tags can trigger a type confusion condition. An attacker can entice a target to visit such a webpage in order to exploit the target machine. Successful exploitation can result in execution of arbitrary code or abnormal termination of Internet Explorer on the target machine.
Strike Microsoft Internet Explorer VBScript Engine String Compare Use After Free	CWE: 119 CVE: 2015-6136 BID: 78538	This strike identifies a vulnerability in Microsoft Internet Explorer. Specifically, the vulnerability occurs with any VBScript function that utilizes a comparison or calculation of two strings. A use after free condition occurs if the function is called with an object as the first parameter, from a class with a default getter which frees the second parameter. If the second parameter is then referenced after being freed memory corruption can occur.
Strike Microsoft Internet Explorer and Edge Memory Corruption	CWE: 119 CVE: 2015-6140	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer and Edge. The vulnerability is due to error while handling certain objects when processing HTML and script code. A remote unauthenticated attacker could exploit these vulnerabilities by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike GE MDS PulseNET Support Account Remote Code Execution Vulnerability	CVE: 2015-6456 BID: 76756	This strike exploits a remote code execution vulnerability in GE MDS PulseNET. The vulnerability is due to improper access granted to hidden support account. An attacker could exploit this vulnerability in order to remotely execute code on the target machine.
Strike GE MDS PulseNET FileDownloadServlet Directory Traversal Vulnerability	CWE: 22 CVE: 2015-6459 BID: 76756	This strike exploits a directory traversal vulnerability in GE MDS PulseNET products. The vulnerability is due to improper validation of parameters when handling requests to FileDownloadServlet. An attacker could exploit this vulnerability in order to gain unauthorized access to information or services.
Strike Unitronics VisiLogic OPLC TeeCommander ActiveX Control Memory Corruption	CWE: 284 CVE: 2015-6478 BID: 77571	This strike identifies a vulnerability in the TeeComander activeX control TeeChart5.ocx. Specifically, a pointer dereference occurs on what is assumed to be a trusted ChartLink method. A different function uses the ChartLink pointer to reference memory in a calculation. If this memory is set to a location we can control, memory corruption can occur and remote code execution is possible.
Strike Ignite Realtime Openfire Cross-Site Scripting (XSS) Vulnerability	CWE: 79 CVE: 2015-6972 EXPLOITDB : 38191	This strike exploits a cross-site scripting (XSS) vulnerability in Ignite Realtime Openfire. The vulnerability is due to improper validation while processing HTTP requests with search parameter. An attacker could exploit this vulnerability in order to run malicious scripts on the target machine.
Strike Safari AppleScript User Assisted Remote Code Execution	CVE: 2015-7007 BID: 77266	This strike exploits a flaw in the Safari Browser on Macintosh Operating Systems (Mac OSX). When a browser is passed an applescript uniform resource locator (URL), it may fail to prompt a user for confirmation before executing script content.
Strike ManageEngine EventLog Analyzer runQuery SQL Injection Vulnerability	CWE: 89 CVE: 2015-7387 EXPLOITDB : 38352 BID: 76866	This strike exploits a sql injection vulnerability in ManageEngine EventLog Analyzer. The vulnerability is due to improper validation of HTTP requests to the runQuery servlet. An attacker could exploit this vulnerability by sending an unauthenticated malicious request to the server, compromising the integrity of the database.
Strike IBM WebSphere Application Server Remote Commons-Collections Code Execution Vulnerability	CWE: 94 CVE: 2015-7450 BID: 77653	This strike exploits a code execution vulnerability in IBM WebSphere Application Server. The vulnerability is due to improper validation of SOAP requests that contain certain serialized objects. An attacker could exploit this vulnerability in order to remotely execute arbitrary code on the target machine.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike ManageEngine OpManager SubmitQuery SQL Injection Vulnerability	CWE: 264  CVE: 2015-7766  EXPLOITDB : 38221  BID: 77047	This strike exploits a sql injection vulnerability in ManageEngine OpManager. The vulnerability is due to improper validation of HTTP requests to the opmapi servlet. An attacker could exploit this vulnerability by sending an unauthenticated malicious request to the server, compromising the integrity of the database.
Strike Unitronics VisiLogic OPLC IPWorksSSL ActiveX Control Memory Corruption	CWE: 94  CVE: 2015-7905  BID: 77571	This strike identifies a vulnerability in the Unitronics VisiLogic's activeX control IPWorksSSL.HTTPS. Specifically, a pointer dereference occurs on what is assumed to be a trusted SSLCertHandle method. If this memory is set to a location we can control, memory corruption will occur and remote code execution is possible.
Strike Schneider Electric ProClima up to 6.1 F1 Bookview buffer overflow	CWE: 119  CVE: 2015-7918  BID: 78421	This strike exploits a memory corruption vulnerability in Schneider Electric ProClima F1BookView ActiveX Control. Specifically the vulnerability in how the Rule and Text parameters are processed as iteration counters in a loop. The loop reads these 2 parameters and calculates their length. Then this data is read onto the stack and if x or y is larger than the amount of data between the current memory location and the end of the stack, a memory access violation occurs.
Strike SearchBlox Multiple Authentication Bypass Vulnerabilities	CWE: 264  CVE: 2015-7919  BID: 78552	This strike exploits multiple authentication bypass vulnerabilities in SearchBlox. The vulnerabilities are due to improper validation of HTTP requests. An attacker could exploit these vulnerabilities in order to add/delete a user, delete a collection, delete reports, import and export the configuration file. By importing and exporting the configuration file, the admin password could be compromised or overwritten and also a crash could be generated.
Strike Samsung SmartViewer STWAXConfigNVR ActiveX Control Remote Code Execution	BID: 77079  CVE: 2015-8039	This strike exploits an out of bounds indexing vulnerability in Samsung SmartViewer STWAXConfigNVR ActiveX control. The flaw is due to the STWAXConfigNVR ActiveX control, which contains an untrusted pointer dereference vulnerability. By enticing a user to visit a malicious web page, arbitrary code can be executed on the client system.
Strike ManageEngine Desktop Central fileupload connectionID Directory Traversal Arbitrary File Upload	CWE: 434  CVE: 2015-8249  EXPLOITDB : 38982	This strike exploits an arbitrary file upload vulnerability in ManageEngine Desktop Central. Files can be uploaded to the target by sending an HTTP POST request to /fileupload with a query parameter action=rds_file_upload. The connectionId parameter is not checked for directory traversal characters. An attacker can send a malicious HTTP POST request to upload an arbitrary file to an arbitrary location on the target system. Successful exploitation may lead to creation or overwriting of arbitrary files, which may lead to execution of arbitrary code with system privileges.

Name	References	Description
Strike Adobe Flash MP3 ID3 Tag Heap BUffer Overflow	BID: 78712 CWE: 119 CVE: 2015-8446	This strike exploits a heap buffer overflow vulnerability in Adobe Flash. The vulnerability is due to a failure when handling malformed MP3 files. Successful exploitation may result in execution of arbitrary code or abnormal termination of the flash process.
Strike IBM SPSS Statistics ActiveX Control Buffer Overflow	BID: 90524 CWE: 119 CVE: 2015-8530	This strike exploits buffer overflow vulnerability within the IBM SPSS Statistics ActiveX Control. This vulnerability is due to lack of boundary checking in the IBM SPSS Statistics ActiveX Control. Remote unauthenticated attackers could exploit this vulnerability to execute arbitrary code on the target system.
Strike Schneider Electric ProClima F1BookView Code Execution	CWE: 119 CVE: 2015-8561 BID: 79802	This strike exploits a memory corruption vulnerability in Schneider Electric ProClima F1BookView ActiveX. The vulnerability is due to insufficient validation of a parameter from the CopyAll method. By enticing a user to access a malicious web page, an attacker could execute code remotely in the context of the affected user.
Strike Microsoft Internet Explorer VBScript and JScript Engine Use After Free	CWE: 119 CVE: 2016-0002 BID: 79894	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically the vulnerability exists when VBScript creates an array and resizes it, and then Javascript code creates an array and references the VBScript code. Later this code is freed, and when another call to the object is made with this freed array as a parameter, which then attempts to dereference a member of this array, it results in a use after free error.
Strike Microsoft Edge Chakra JavaScript Engine Integer Overflow	BID: 79891 CWE: 119 CVE: 2016-0024	This strike exploits an integer overflow vulnerability in Microsoft Edge's Chakra JavaScript engine. Specifically the vulnerability is due to improper bounds checking when creating a DataView object. If an overly large value is given as the byteLength variable, an integer overflow can occur when calculating the DataView range. This can potentially be leveraged by an attacker to disclose information or corrupt memory.
Strike Microsoft Silverlight Decoder Code Execution	CWE: 20 CVE: 2016-0034	This strike exploits a vulnerability in Microsoft Silverlight. The vulnerability is due to a buffer overflow while calling GetChars method. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in execution of arbitrary code or abnormal termination of the Silverlight application.
Strike Microsoft Internet Explorer CDomPrototype Object Memory Corruption	CWE: 119 CVE: 2016-0063 BID: 82658	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically a type confusion vulnerability exists when a DomPrototype object is allocated and assigned to a local variable. If the variable is changed to reference a different pointer later and then eventually called, an access violation occurs because it believes it is still an object of type CDomPrototype. When this happens memory corruption occurs which can lead to remote code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Edge WebNotes Same-Origin Policy Bypass	CWE: 254  CVE: 2016-0161	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, it is possible to open a script that uses a javascript origin to then retrieve a file origin resource. This type of cross origin file read should not be possible (as it violates the same-origin policy). However, if a user can be tempted to use the Edge browser's Web Note functionality in a certain manner, this is bypass becomes possible.
Strike Microsoft Internet Explorer Scripting Engine Use After Free Condition	BID: 90012  CWE: 119  CVE: 2016-0189	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically, the vulnerability exists in the VBScript and JavaScript scripting engines. When creating an array in VBScript, heap memory is allocated. When this array size is then later changed, this structure is cleared or freed, however a pointer to this object still remains. It is possible to then access this object causing a use after free condition to occur which results in memory corruption. This type of memory corruption may lead to a denial of service or even remote code execution.
Strike Oracle Application Testing Suite DownloadServlet TMAPReportImage Parameter Directory Traversal	CVE: 2016-0480  BID: 81070	This strike exploits a directory traversal vulnerability in Oracle Application Testing Suite. The vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability in order to download arbitrary files.
Strike Oracle Application Testing Suite Directory Traversal	CVE: 2016-0481  BID: 81184	This strike exploits a directory traversal vulnerability in Oracle Application Testing Suite. The vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability in order to download arbitrary files.
Strike Oracle Application Testing Suite DownloadServlet scriptPath Parameter Directory Traversal	CVE: 2016-0484  BID: 81102	This strike exploits a directory traversal vulnerability in Oracle Application Testing Suite. The vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability in order to download arbitrary files.
Strike Oracle Application Testing Suite ReportImage Directory Traversal Arbitrary File Upload	CVE: 2016-0489  BID: 81184	This strike exploits a directory traversal vulnerability in Oracle Application Testing Suite. The vulnerability is due to improper validation of HTTP request. An attacker could exploit this vulnerability in order to upload arbitrary files.
Strike Oracle Application Testing Suite Directory Traversal Arbitrary File Upload	CVE: 2016-0490  BID: 81173	This strike exploits a directory traversal vulnerability in Oracle Application Testing Suite. The vulnerability is due to improper validation of HTTP request. An attacker could exploit this vulnerability in order to upload arbitrary files.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle Application Testing Suite UploadFileUpload Directory Traversal	CVE: 2016-0491 BID: 81169	This strike exploits a directory traversal exploit in Oracle Application Testing Suite. HTTP POST requests to /olt/UploadFileUpload.do do not sanitize for directory traversal characters. An authenticated attacker can send a specially crafted HTTP POST request to upload arbitrary files to any location writable by the Oracle Load Testing service. Note, while this attack requires authentication, it can be paired with the authentication bypass attack, CVE-2016-0492.
Strike Oracle Application Testing Suite Authentication Bypass	CWE: 23 CVE: 2016-0492	This strike exploits an authentication bypass vulnerability in Oracle's Application Testing Suite. The vulnerability is in the isAllowedUrl function which checks for url starting with certain hard coded strings. A remote attacker can exploit this vulnerability by sending crafted request to the vulnerable server. Successful exploitation allows attacker to gain unauthenticated access to affected product.
Strike Apache Jetspeed PageManagementService Persistent XSS	CWE: 79 CVE: 2016-0711	This strike exploits a cross site scripting vulnerability in Apache Jetspeed. Specifically a persistent XSS exists in the updateNodeInfo method of the PageManagementService. The title parameter is not properly sanitized, and an authenticated user can inject javascript via an HTTP request method.
Strike Apache Jetspeed Portal URI Path XSS	CWE: 79 CVE: 2016-0712	This strike exploits an XSS vulnerability in Apache Jetspeed. Specifically the url path is not properly sanitized, and code can be injected into the Help, About, Print, Minimize and Maximize icons. This strike grabs user form fields and alerts them to the user. However, it is possible to load a completely fake form, grab these values and send them to a remote attacker.
Strike Ruby Rails Dynamic Render Directory Traversal	CWE: 22 CVE: 2016-0752	This strike exploits a Directory Traversal vulnerability in the web component of Ruby Rails. The vulnerability is due to unrestricted use of the render method. A remote unauthenticated attacker could exploit this vulnerability by sending a crafted request. Successful exploitation could result in unauthorized file access and leakage of sensitive data.
Strike Jenkins CI Server createItem and createView Insecure Deserialization Command Execution	CWE: 20 CVE: 2016-0792	This strike exploits a command execution vulnerability in Jenkins CI Server. POST requests to /createView or /createItem containing serialized java.util.map objects will be deserialized. An attacker can craft a serialized object to contain an arbitrary command. Successful exploitation will lead to arbitrary command execution.
Strike Advantech WebAccess Dashboard Multiple File Upload Vulnerabilities	CVE: 2016-0854 BID: 80745 EXPLOITDB : 39735	This strike exploits a file upload vulnerability in Advantech WebAccess. WebAccess has several URIs designed to accept image files. These files are not verified, and specially crafted HTTP POST requests can be used to upload any arbitrary file. This includes uploading asp and aspx files, which can then be called to achieve arbitrary asp code execution with the privileges of the IIS service. Successful exploitation may result in creation of arbitrary files and could lead to arbitrary code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Advantech WebAccess FileAjaxAction removeFolder Directory Traversal	CWE: 22 CVE: 2016-0855 BID: 80745	This strike exploits a directory traversal vulnerability in Advantech WebAccess. WebAccess has a removeFolder function which deletes a folder and its contents. It does not sanitize for directory traversal characters. An attacker can send a specially crafted HTTP request to delete arbitrary directories on the target system.
Strike Adobe Flash H264 File Stack Corruption	CWE: 119 CVE: 2016-0967 EXPLOITDB : 39466 GOOGLE: 633	This strike exploits a remote code execution vulnerability in Adobe Flash Player. The vulnerability is due to a stack corruption when Adobe flash loads the FLV file. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in abnormal termination of the flash process.
Strike Adobe Flash Zlib Codec Heap Overflow	CWE: 119 CVE: 2016-1001 EXPLOITDB : 39609 GOOGLE: 720 BID: 84310	This strike exploits a remote code execution vulnerability in Adobe Flash Player. The vulnerability is due to a heap overflow in the Zlib codecs used when playing FLV files in flash. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in execution of arbitrary code or abnormal termination of the flash process.
Strike PHPMailer Sender Field Command Injection	CWE: 77 CVE: 2016-10033 BID: 95108	This strike exploits a command injection vulnerability in PHPMailer. The sender field is used as a PHP parameter. The field allows space characters to be escaped by using a double quote character. By escaping additional spaces, additional parameters can be injected, which will then be evaluated. An attacker can use this to insert arbitrary parameters to be evaluated, including the -X parameter to write out a log with arbitrary php code, which can then be executed.
Strike PHPMailer Sender Field Improper Patch Command Injection	CWE: 77 CVE: 2016-10045 BID: 95130	This strike exploits an incomplete patch for a command injection vulnerability in PHPMailer. The sender field is used as a PHP parameter. The field originally allowed space characters to be escaped by using a double quote character. By escaping additional spaces, additional parameters can be injected, which will then be evaluated. The patch added escapeshellarg() escaping to prevent this attack. However, this escaping clashes with escapeshellcmd() escaping, which happens later. Due to this clash, the single quote character can be used to achieve the same result on a patched machine. An attacker can use this to insert arbitrary parameters to be evaluated, including the -X parameter to write out a log with arbitrary php code, which can then be executed.

Name	References	Description
Strike PHP phar_parse_pharfile filename_len Integer Overflow	BID: 95774  CWE: 190  CVE: 2016-10159	This strike causes a denial of service in PHP due to a integer overflow when parsing a phar file. The flaw is a bounds check for the filename length field embedded in the file. A malicious file can cause a PHP server to crash.
Strike NETGEAR WNR2000v5 Router hidden_lang_avi Buffer Overflow Vulnerability	CVE: 2016-10174  CWE: 120	This strike exploits a buffer overflow vulnerability in NETGEAR WNR2000v5 Router. The vulnerability is due to a buffer overflow in the hidden_lang_avi parameter when handling HTTP requests to the '/apply.cgi?/lang_check.html' endpoint. An unauthenticated remote attacker could exploit this vulnerability by sending a crafted HTTP request to execute arbitrary OS commands, potentially leading to remote code execution.
Strike D-Link DCS-930L firmware OS Command Injection	CWE: 78  CVE: 2016-11021	This strike exploits an OS Command Injection Vulnerability in D-Link Devices. The vulnerability is due to improper sanitization of user supplied parameter. A remote authenticated attacker could exploit this by sending a crafted packet and might result in remote code execution in the context of root user.
Strike Adobe Flash Out of Bounds When Placing Object	CVE: 2016-1104  BID: 90618  EXPLOITDB : 39825  GOOGLE: 794	This strike exploits a remote code execution vulnerability in Adobe Flash Player. The vulnerability is due to an out of bounds read when placing a corrupt image. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in abnormal termination of the flash process.
Strike NETGEAR Management System NMS300 File Upload Vulnerability	CVE: 2016-1524  BID: 82630	This strike exploits a file upload vulnerability in NETGEAR Management System NMS300. The vulnerability is due to improper unauthenticated access to certain URLs that allow uploading of files and then accessing them. By exploiting this vulnerability an attacker could upload and execute code on the target machine.
Strike NETGEAR Multiple WAP Devices macAddress Command Injection Vulnerability	CWE: 77  CVE: 2016-1555	This strike exploits an OS command injection vulnerability in Netgear Devices. The vulnerability arises due to improper sanitization of user-supplied input in specific PHP scripts, such as boardData102.php, boardData103.php, boardDataNA.php, boardDataJP.php, and boardDataWW.php. A remote, unauthenticated attacker can exploit this vulnerability by injecting commands through the macAddress parameter in these scripts. Successful exploitation of this vulnerability could lead to arbitrary command execution.

Name	References	Description
Strike Novell Service Desk LiveTime File Upload Directory Traversal	CWE: 22 CVE: 2016-1593	This strike exploits a directory traversal vulnerability in Novell Service Desk. Service Desk allows administrators to upload CSV files, however Service Desk fails to validate the file is actually a CSV and does not sanitize for directory traversal characters. An authenticated user could exploit this in order to upload arbitrary files to arbitrary locations. Additionally, Service Desk contains default administrator credentials, which could be used by an attacker to gain authentication.
Strike Hewlett Packard Enterprise Vertica Management Console validateAdminConfig Remote Code Execution	CWE: 77 CVE: 2016-2002	This strike identifies a vulnerability in HP Enterprise Vertica Management Console. Specifically an un-authenticated user is able to perform command injection by sending an HTTP request to the validateAdminConfig URI. The code does not properly sanitize the McPort parameter. However, because it is checked with a command line utility, a user is able to inject and execute shell commands remotely.
Strike Apache Jetspeed User Manager Services REST API Unauthorized Access	CWE: 264 CVE: 2016-2171	This strike exploits a vulnerability in Apache Jetspeed. Specifically the User Manager services allow for unauthorized access via the REST API. Any user is able to query the users directory to create and delete users without having to authenticate via the REST API.
Strike SAP NetWeaver J2EE Engine UDDISecurityImplBean SQL Injection	CWE: 89 CVE: 2016-2386	This strike exploits a SQL injection vulnerability in the web service interface of SAP NetWeaver. The vulnerability is due to insufficient input sanitization in the UDDISecurityImplBean endpoint, specifically within the permissionId parameter of the deletePermissionById method. A remote unauthenticated attacker could exploit this flaw by injecting malicious SQL statements into a SOAP request. Successful exploitation allows the attacker to enumerate sensitive backend data, such as administrative user information and hashed credentials.
Strike Squid Vary Header Long String Denial of Service	CWE: 20 CVE: 2016-2569 BID: 83406	This strike exploits a denial of service vulnerability in Squid Proxy Server. The Vary header consists of comma delimited values. The server expands this header into a comma + space delimited string. This expansion may cause the string to exceed the maximum character limit, which will result in an assertion failure, terminating the Squid process. Successful exploitation will result in abnormal termination of the Squid process, leading to a denial of service condition.
Strike CMS Made Simple Web Server Cache Poisoning	CWE: 79 CVE: 2016-2784 EXPLOITDB : 39760	This strike exploits a vulnerability in CMS Made Simple. CMS Made simple is a content management system that runs on a web server, and helps in creating web sites. A vulnerability exists in how HTTP requests are parsed. Specifically the Host header is not properly validated, and a maliciously crafted header can allow for the Web Server cache to be poisoned. This kind of vulnerability can be leveraged by other kinds of attack vectors like Cross site scripting injection as well as server re-directs.
Strike GD Library libgd gd_gd2 c Heap Buffer Overflow	CWE: 189 CVE: 2016-3074	A heap buffer overflow vulnerability has been reported in libgd. The vulnerability is due to a signedness error that leads to a heap buffer overflow. Libgd is included within PHP. A remote attacker can exploit this flaw having the target process a crafted malicious GD2 file. Successful exploitation could result in code execution in the security context of the user process.

Name	References	Description
Strike Apache Struts Remote Command Execution	BID: 87327 BID: 91787 CWE: 77 CVE: 2016-3081	This strike exploits a remote command execution vulnerability in Apache Struts. An HTTP request with a specially crafted chained expression can be used to execute arbitrary commands. Successful exploitation may result in command execution.
Strike Shopware getTemplateName File Inclusion and Information Disclosure	BID: 97979 CWE: 20 CVE: 2016-3109	This strike exploits a vulnerability in Shopware. Specifically the vulnerability exists in the way the getTemplateName function fails to sanitize input when building the file path and name. If a request is made containing the f or file parameters with directory traversal characters in place a file information disclosure may be possible. This strike illustrates the information disclosure vulnerability, however, due to the nature of the disclosed vulnerability remote code execution may also be possible.
Strike Microsoft Internet Explorer Javascript Library TypedArray Use After Free	BID: 91106 CWE: 119 CVE: 2016-3210	This strike exploits a use after free vulnerability in Microsoft Internet Explorer's Javascript library. Specifically when creating a TypedArray - Array Buffer object with any of the array constructors as a view, and then sending that object as an argument of a worker script message, a use after free condition can occur. This results in memory corruption and can lead to a denial of service or potentially remote code execution.
Strike Microsoft Edge isEqualNode Memory Corruption	CWE: 119 CVE: 2016-3222 BID: 91094	This strike exploits a vulnerability in the Microsoft Edge Browser. Specifically, the vulnerability exists in the isEqualNode method. An uninitialized local variable used by another function and is later dereferenced, leading to memory corruption. This memory corruption can potentially result in remote code execution or a denial of service condition in the application.
Strike Microsoft Edge TextNode Unicode Character Information Disclosure	BID: 91599 CWE: 284 CVE: 2016-3244	This strike exploits a vulnerability in Microsoft Edge. The vulnerability is due to how UTF encoded characters are handled inside a TextNode object. When these characters are processed the TextNode content's size is not calculated correctly. This incorrect value can then lead to disclose memory information that may lead to the bypass of certain protection mechanisms like ASLR.
Strike Microsoft Internet Explorer and Edge Browser White-space Style Property Memory Corruption	CVE: 2016-3247 BID: 92828	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer and Edge Browsers. Specifically, when the white-space style property of an element is set to pre-line and the element includes a carriage return, an out-of-bound memory read occurs. An attacker can potentially take advantage of this vulnerability to execute code remotely on the target system.

Name	References	Description
Strike Microsoft Internet Explorer and Edge Browser ResProtocol Information Disclosure	CWE: 200 CVE: 2016-3267 BID: 93376	This strike exploits an information disclosure vulnerability in the Microsoft Internet Explorer and Edge Browsers. It is possible for an attacker to attach a readyStateChange event handler to an iframe in such a way that allows information about a Portable Executable file to be disclosed to the user via the Res protocol URI.
Strike Microsoft Internet Explorer Cblob Object Use-After-Free	CWE: 119 CVE: 2016-3288 BID: 92321	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically in Internet Explorer version 11 a Use-After-Free vulnerability exists in the way the browser handles Cblob objects. A FileReader object is created, and then reads a Cblob object in a specific way. If the garbage collector is then called and this freed object is referenced a use after free condition occurs. This leads to a denial of service in the browser, and can potentially lead to remote code execution.
Strike Microsoft Internet Explorer Internet Messaging API Information Disclosure	CWE: 200 CVE: 2016-3298 BID: 93392	This strike exploits an information disclosure vulnerability in Microsoft Internet Explorer. Specifically, when the loadXML function is called on an MSXML DOMDocument with URI set to a malicious MHTML URI, it is possible to discern whether or not a file exists on the target system through errors that are reported back to the user of whether or not that file exists. A malicious user can use abuse this functionality to disclose this information about the target user's system.
Strike Microsoft Internet Explorer and Edge HTTP Continue Response Information Disclosure	BID: 92832 CWE: 200 CVE: 2016-3325	This strike exploits an information disclosure vulnerability in Microsoft Internet Explorer and Edge. An attacker can craft a malicious HTTP Continue response message and cause an out of bounds read condition in the victim's browser. This can potentially lead to an information disclosure.
Strike Microsoft Internet Explorer and Edge Browser Scripting Engine Type Confusion	CWE: 119 CVE: 2016-3382 BID: 93386	This strike exploits a vulnerability in the Microsoft Internet Explorer and Edge Browser's Chakra Scripting Engine. The vulnerability is due to the scripting engine's VarToDispEx function using the ActivationObjectEx object as a pointer to a different javascript function. If this function pointer is assigned to an eval function it is possible to cause type confusion to occur when later referencing this ActivationObjectEx function.
Strike Microsoft Internet Explorer VBScript Join Type Confusion	CWE: 119 CVE: 2016-3385 BID: 93397	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically, a type confusion vulnerability exists in the Microsoft scripting engine's Join function. A malicious attacker can craft code in such a way that when Join is called upon an array object after its contents have been changed, the reference to the original object is kept. If the type of the object in the array has changed it will result in type confusion. It may also be possible to cause a denial of service condition in the browser or achieve remote code execution by corrupting these memory contents in a specified manner.

Name	References	Description
Strike Microsoft Edge CallSpreadFunction Memory Corruption	CWE: 119 CVE: 2016-3386 BID: 93426 EXPLOITDB : 40605	This strike exploits a vulnerability in Microsoft Edge. Specifically if the spread operator is used on an array, the CallSpreadFunction calls spreadArgs in an attempt to split each element into objects. If the length of this array is altered while a different object maintains a reference to this array, the spread operator does not update the new length. An attacker can craft javascript in such a manner that will cause memory corruption to occur, causing a denial of service in the browser and potentially leading to remote code execution.
Strike Adobe Flash ATF Processing Heap Overflow	CVE: 2016-4135 GOOGLE: 786	This strike exploits a remote code execution vulnerability in Adobe Flash Player. The vulnerability is due to a heap overflow in ATF processing. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in execution of arbitrary code or abnormal termination of the flash process.
Strike Adobe Flash Player AVC Decoding Memory Corruption	BID: 92930 CWE: 119 CVE: 2016-4275 EXPLOITDB : 40421 GOOGLE: 859	This strike exploits a remote code execution vulnerability in Adobe Flash Player. There is a memory corruption occurs when freeing memory after AVC decoding. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in execution of arbitrary code or abnormal termination of the flash process.
Strike SolarWinds SRM Profiler Multiple SQL Injections	CWE: 89 CVE: 2016-4350	This strike exploits multiple SQL injection vulnerabilities in SolarWinds SRM Profiler. It is possible for a remote authenticated attacker to send an HTTP request to one of several URIs on the Resource monitor that allow for them to inject and execute arbitrary SQL commands via multiple vulnerable parameters per URI. Default Administrator credentials are known and make this attack easily executed remotely.
Strike Apache Struts URLValidator Forward Slashes Denial of Service	CWE: 20 CVE: 2016-4465 BID: 91278	This strike exploits a denial of service vulnerability in Apache Struts. The URLValidator class improperly handles URLs with many forward slash characters during validation. The improper handling leads to resource exhaustion. An attacker can send a specially crafted HTTP request which to a Struts application which accepts URLs as a parameter to exploit this vulnerability. Successful exploitation may result in a denial of service condition.
Strike Trihedral VTScada Wap Filter Bypass	CWE: 287 CVE: 2016-4510 BID: 91077	This strike exploits a filter bypass vulnerability in Trihedral VTScada. Specifically, the VTScada application allows for an un-authenticated user to send http requests to access files with one of several valid file extensions. However, if a null byte character is included with the valid file extension the application processes the string but truncates the file path at the null character. This allows a remote attacker to disclose file information that is not meant to be seen by external users.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Schneider Electric SoMachine HVAC ActiveX Control Memory Corruption	CVE: 2016-4529 BID: 91778	This strike exploits a pointer dereference vulnerability in Schneider Electric's SoMachine HVAC software. Specifically the SetDataIntf method in the AxEditGrid activeX control can be used by an attacker to corrupt memory. This memory corruption can lead to a denial of service condition or possible remote code execution.
Strike Trihedral VTScada Wap Directory Traversal	CWE: 22 CVE: 2016-4532 BID: 91077	This strike exploits a directory traversal vulnerability in Trihedral VTScada. When an un-authenticated user pairs this attack with CVE-2016-4510 ,which allows for a file to specified with the inclusion of a null character, directory traversal characters can be added to the file name and get interpreted as the file path. This allows a remote attacker to effectively traverse the applications directory structure and read documents at will.
Strike Squid Proxy ESI Response Processing Denial of Service	CVE: 2016-4555 CWE: 20	This strike exploits a denial of service vulnerability in the Edge Side Includes (ESI) component of the Squid proxy. The vulnerability is due to incorrect pointer handling when processing ESI responses. A remote attacker could exploit this vulnerability by sending crafted ESI response data to the target system. Successful exploitation allows the attacker to cause a denial of service condition for all clients accessing the Squid service. Note: This strike simulates the request coming from the Squid Proxy to the attacker controller server.
Strike Google Chrome Blink Component Integer Overflow	CWE: 119 CVE: 2016-5182 BID: 93528	This strike exploits a vulnerability in the Google Chrome Blink component. The vulnerability is due to an integer overflow that occurs in the ImageBitmap function when processing a createImageBitmap function with overly large width and height values. When the ImageBitmap function copies these values into a heap buffer an overflow can occur. This can potentially allow for remote code execution.
Strike Symantec Web Gateway Whitelist white_ip Command Execution	CWE: 78 CVE: 2016-5313 BID: 93284	This strike exploits a command execution vulnerability in Symantec Web Gateway. Authenticated requests to the URI / spywall/new_whitelist.php are used to create whitelists. The parameter white_ip is not validated if the sid parameter is non-zero. The value of white_ip will later be used in a shell command, allowing for arbitrary command execution with administrative privileges. An authenticated attacker could send specially crafted HTTP messages to achieve arbitrary command execution with administrative privileges.
Strike Micro Focus GroupWise Post Office Agent Buffer Overflow	CWE: 190 CVE: 2016-5762 BID: 92642	This strike exploits a vulnerability in Micro Focus GroupWise Post Office Agent. An integer overflow can lead to a heap buffer overflow in the GroupWise Post Office Agent. If an unauthenticated user sends a login request with an overly large username or password to the agent a buffer is overflowed. This then leads to a denial of service condition, and can potentially allow for remote code execution to occur.

Name	References	Description
Strike EPIC MyChart - X-Path Injection	CWE: 91 CVE: 2016-6272 EXPLOITDB : 44098	This strike exploits a SQL injection vulnerability in the Epic Systems Corporation MyChart. This vulnerability is due to improper sanitization for the GE parameter "topic". A remote attacker can access contents of an XML document containing static display strings, such as field labels on the target system.
Strike Netgear R7000 Router CGI Command Injection	CWE: 352 CVE: 2016-6277 BID: 94819 EXPLOITDB : 40889	This strike exploits a command execution vulnerability in Netgear R7000 Router Web Interface. The vulnerability is due to improper access checks of the web platform resources. Successful exploitation can result in arbitrary commands via shell metacharacters in the path info to 'cgi-bin'.
Strike WordPress Admin API Directory Traversal	CWE: 22 CVE: 2016-6896	This strike exploits a directory traversal vulnerability inside WordPress. Specifically this occurs when HTTP requests are sent to the admin-ajax page with the action parameter update-plugin set. Directory traversal characters are not handled properly, and an authenticated user can send multiple requests to this API, which will result in a denial of service condition.
Strike FortiOS Cookie Parser Buffer Overflow Vulnerability	CWE: 119 CVE: 2016-6909 BID: 92523 EXPLOITDB : 40276	This strike exploits a buffer overflow vulnerability in FortiGate firmware (FortiOS). The vulnerability is due to failure to sanitize user-supplied input while parsing an HTTP request. An remote, unauthenticated attacker could exploit this vulnerability to remotely execute arbitrary code on the target system. NOTE: A publicly available exploit for this vulnerability can be found in the reported leak of 0Day exploits from the NSA by a group known as the "Shadow Brokers", identified as EGREGIOUSBLUNDER.
Strike Microsoft Edge Browser Chakra Engine Array.map Type Confusion	CWE: 119 CVE: 2016-7190 BID: 93428	This strike exploits a vulnerability in the Microsoft Edge Browser. Specifically, a type confusion vulnerability exists in the Microsoft Edge module Chakra.dll. A malicious attacker can craft javascript in such a way that when a proxy object is created and Array.map is called upon that object, memory information can be disclosed. It may also be possible to cause a denial of service condition in the browser or achieve remote code execution by corrupting these memory contents in a specified manner.
Strike Microsoft Edge Browser Chakra Engine TemplatdForEachItemInRange Type Confusion	CWE: 119 CVE: 2016-7194 BID: 93399	This strike exploits a vulnerability in the Microsoft Edge Browser. Specifically, a type confusion vulnerability exists in the Microsoft Edge module Chakra.dll. A malicious attacker can craft javascript in such a way that when the TemplatdForEachItemInRange method is called on an array believing it is of type int, the method will disclose memory contents of the non-integer object in the array.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer and Edge Browsers CLSIDFromHtmlString Function Information Disclosure	CWE: 119 CVE: 2016-7195 BID: 94052	This strike exploits a vulnerability in the Microsoft browsers Edge and Internet Explorer. When the object element's classid parameter is parsed and found to not contain the "clsid:" string, and the characters of this string are non printable, it is possible to read out-of-bounds memory. This can result in a denial of service condition in the browser, or potentially disclose memory contents that may lead to an ASLR bypass.
Strike Microsoft Edge Browser Array.filter Information Disclosure	CWE: 119 CVE: 2016-7200 BID: 93968 GOOGLE: 922	This strike exploits a vulnerability in the Microsoft Edge Browser. Specifically, in the Chakra javascript engine, it is possible to corrupt memory due to the way that the filter function assumes the destination array is of a certain type, and can end up writing a pointer to an integer array. It is then possible to disclose this pointer information, and it is also possible to corrupt memory in such a way that may cause a denial of service condition in the browser or potentially allow for remote code execution to occur.
Strike Microsoft Edge Browser Chakra Engine Array.shift Type Confusion	CWE: 119 CVE: 2016-7201 BID: 94038	This strike exploits a vulnerability in the Microsoft Edge Browser. Specifically, a type confusion vulnerability exists in the Microsoft Edge module Chakra.dll. A malicious attacker can craft javascript in such a way that when the Array.shift method is called on an array believing it is always of a certain type, type confusion can occur. This may allow for an attacker to disclose memory contents or potentially execute remote code.
Strike Microsoft Edge Visited Link Information Disclosure	CWE: 79 CVE: 2016-7206 BID: 94737	This strike exploits an information disclosure vulnerability in Microsoft Edge. By utilizing the webkitTextFillColor property an attacker can discern whether or not a link exists in the user's history, and has been visited.
Strike Microsoft Edge Chakra JavaScript Engine EntryEvalHelper Function Memory Corruption	CWE: 119 CVE: 2016-7240 BID: 94046 GOOGLE: 948	This strike exploits a vulnerability in Microsoft Edge. Specifically if an eval function is called from a Proxy object, the EntryEvalHelper function does not properly verify the internal arguments and they get converted to objects of a different type. This creates a type confusion vulnerability. An attacker can craft javascript in such a manner that will cause memory corruption to occur, causing a denial of service in the browser and potentially leading to remote code execution.
Strike Microsoft Edge Browser Chakra Engine JavascriptArray DirectSetItemAt Type Confusion	CWE: 119 CVE: 2016-7242 BID: 94041	This strike exploits a vulnerability in the Microsoft Edge Browser. Specifically, a type confusion vulnerability exists in the Microsoft Edge module Chakra.dll. A malicious attacker can craft javascript in such a way that when the DirectSetItemAt method is called on an array believing it is of type int, type confusion occurs. This may allow for an attacker to disclose memory contents or potentially execute remote code.

Name	References	Description
Strike Microsoft Internet Explorer CWigglyShape DrawMultiple Memory Corruption	CWE: 119 CVE: 2016-7283 BID: 94726	This strike exploits a vulnerability in the Microsoft Internet Explorer Browser. Specifically, in the CWigglyShape DrawMultiple function a loop is created that draws a segment of a Unicode character during each iteration through the loop. It is possible to corrupt the loop counter causing the loop to not terminate properly and allowing for an out of bounds memory read. This memory corruption can lead to an information disclosure or cause a denial of service condition to occur in the browser, and it may also be possible for remote code execution to occur.
Strike Microsoft Edge SIMD Object toLocaleString Memory Corruption	CWE: 119 CVE: 2016-7286 BID: 94748	This strike exploits a vulnerability in the Microsoft Edge Browser. Specifically, when the toLocaleString function is called on a SIMD object, uninitialized memory is used to convert numbers to the locale, resulting in memory corruption. This can cause a denial of service condition to occur in the browser, or potentially lead to remote code execution.
Strike Trend Micro Threat Discovery Appliance Policy Upload Information Disclosure	CWE: 361 CVE: 2016-7547 BID: 97610	This strike exploits a vulnerability in Trend Micro's Threat Discovery Appliance. Specifically, a post authentication file disclosure vulnerability exists when using the timezone parameter in the admin_sys_time.cgi interface. A malicious user can dump file contents as the root user when logged in. This exploit can be used in conjunction with CVE 2016-7552, the Trend Micro Threat Discovery Appliance authentication bypass vulnerability, to gain access to the device.
Strike Trend Micro Threat Discovery Appliance Directory Traversal Authentication Bypass	CWE: 22 CVE: 2016-7552 BID: 97599	This strike exploits a directory traversal vulnerability in Trend Micro's Threat Discovery Appliance. A pre-authenticated attacker can send an HTTP request to the device allowing for a configuration file to be deleted. This action may cause of denial of service, and when the server is rebooted, the login password is reset to the default, thus bypassing authentication and allowing the attacker to login.
Strike McAfee ePolicy Orchestrator DataChannel SQL Injection	CWE: 89 CVE: 2016-8027 BID: 95981	An SQL injection vulnerability exists in McAfee ePolicy Orchestrator. The vulnerability is due to insufficient input validation. The successful exploitation of this vulnerability can result in database information disclosure without authentication via a specially crafted HTTP POST request.
Strike Brocade Network Advisor FileReceiveServlet filename Directory Traversal	CWE: 22 CVE: 2016-8204	This strike exploits a directory-traversal vulnerability in Brocade Network Advisor. The vulnerability is due to lack of input-validation on the filename parameter for FileReceiveServlet. A remote attacker could exploit this vulnerability to upload arbitrary files and result in arbitrary code execution with privileges of the SYSTEM.
Strike Brocade Network Advisor DashboardFileRecei veServlet Directory Traversal Vulnerability	CVE: 2016-8205	This strike exploits a directory traversal vulnerability in Brocade Network Advisor. The vulnerability resides in the DashboardFileReceiveServlet servlet due to insufficient input validation of the filename parameter in HTTP multipart form requests. A remote, unauthenticated attacker could exploit this vulnerability to upload malicious files, potentially leading to arbitrary code execution with SYSTEM privileges.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Brocade Network Advisor CliMonitorReportServlet FILENAME Directory Traversal	BID: 95691 CWE: 22 CVE: 2016-8207	This strike exploits a directory-traversal vulnerability in Brocade Network Advisor. The vulnerability is due to lack of input-validation on the FILENAME parameter. A remote attacker could exploit this vulnerability to read arbitrary files from the targeted system.
Strike Joomla Account Creation Security Bypass	CWE: 20 CVE: 2016-8869 BID: 93883 EXPLOITDB : 40637	This strike exploits an account creation security bypass in Joomla. The vulnerability is due to improper validation of HTTP POST data to index.php/component/users. An attacker could exploit this vulnerability in order to create an account on the target server.
Strike Joomla Privilege Escalation Vulnerability	CWE: 20 CVE: 2016-8870 BID: 93876 EXPLOITDB : 40637	This strike exploits a privilege escalation vulnerability in Joomla. The vulnerability is due to improper validation of HTTP POST data to index.php/component/users. An attacker could exploit this vulnerability in order to create an admin account on the target server.
Strike Mozilla Firefox SVG Animation NotifyTimeChange Use After Free	CWE: 416 CVE: 2016-9079 BID: 94591	This strike exploits a use-after-free vulnerability in the Mozilla Firefox and Tor Browsers on the Windows platform. Specifically the vulnerability exists in the SVG animation function nsSMILTimeContainer::NotifyTimeChange(). This is a remote code execution vulnerability in Firefox Browser versions less than 50.0.2. A vulnerable version of the application can run code of the attacker's choosing at will.
Strike Microsoft Edge Same Origin Bypass Information Disclosure	CVE: 2017-0002 BID: 95284	This strike exploits a policy bypass vulnerability in the Microsoft Edge Browser. Specifically, a domainless page is not prevented from modifying another domainless page even if they are from different domains. A redirect loads a website from a different domain. If this site contains an empty iframe, the code embedded within the URL, that is used to perform the redirect, will inject code into this empty iframe. This achieves code execution and allows for remote information disclosure across a different domain. This is also achievable if the site does not contain an empty iframe. In this case the code in the URI creates an empty frame first by modifying an existing iframe and injects code into that iframe.
Strike Microsoft Edge Getter Use After Free	CWE: 416 CVE: 2017-0070 BID: 96690	This strike exploits a vulnerability that exists in Microsoft Edge. An attacker can craft Javascript in a way that causes a Use After Free condition to occur when the NativeCodeGenerator::CheckCodeGenThunk function is called on a pointer that has had its memory freed. This can cause a denial of service in the browser or potentially allow for remote code execution to occur.

Name	References	Description
Strike Microsoft Internet Explorer JoinToString Function Type Confusion	CWE: 119 CVE: 2017-0130 BID: 96647	This strike exploits a vulnerability in Microsoft Internet Explorer. Specifically, an attacker can craft javascript in such a way that overwrites the eval method and calls the Javascript function JoinToString with an object that is not of the expected writeableString type. This causes type confusion to occur and can lead to a denial of service condition in the browser or potentially remote code execution.
Strike Oracle GlassFish OSE Path Traversal	CWE: 22 CVE: 2017-10000 28 EXPLOITDB : 39441	This strike exploits a directory traversal found in GlassFish open source Java EE project. The vulnerability is due to insufficient user input sanitization passed through the URI, addressing various resources. A specially crafted HTTP GET request could allow an attacker to read arbitrary files from the file system.
Strike Primetek Primefaces Padding Oracle Remote Code Execution	CWE: 326 CVE: 2017-10004 86	This strike exploits a command injection vulnerability in the web component of Primetek Primefaces. The vulnerability is due to inadequate encryption strength. A remote attacker could exploit this vulnerability by sending a crafted request using the known password or the default password. Successful exploitation could result in arbitrary command execution under the security context of the root user.
Strike Oracle WebLogic Server WorkContextXmlInputAdapter Insecure Deserialization - RCE	CVE: 2017-10271 BID: 101304	An insecure deserialization vulnerability was found in Oracle WebLogic Server due to insufficient validation of serialized XML data. Vulnerability can be exploited by sending a specially crafted serialized object. Successful exploitation can result in arbitrary code execution in the context of the user running WebLogic.
Strike IBM Informix Dynamic Server heap buffer overflow	CVE: 2017-1092 BID: 98615	This strike exploits a heap buffer overflow in IBM Informix Dynamic Server heap buffer overflow. The vulnerability is due to lack of input validation of HTTP post request to index.php. This vulnerability could allow an unauthorized user to execute arbitrary code as system admin on Windows servers
Strike IBM Informix Open Admin welcomeService Command Execution	CVE: 2017-1092	An input validation vulnerability has been found in IBM Informix Open Admin Tool. The vulnerability is due to improper parsing of user-supplied input to the SOAP interface. Successful exploitation can result in arbitrary code execution in the security context of the SYSTEM user.
Strike YAWS Unauthenticated Remote File Disclosure	CWE: 22 CVE: 2017-10974 BID: 99515 EXPLOITDB : 42303	This strike exploits a local file information disclosure vulnerability in YAWS application. The root cause of this flaw is a directory traversal vulnerability. The vulnerability is due to invalidation of user input sent in requested URLs. Successful exploitation will allow an attacker to obtain sensitive information from the server, including SSL private key, configuration files and access logs.

Name	References	Description
Strike Synology Photo Station Arbitrary File Upload	CWE: 287 CVE: 2017-11151 EXPLOITDB : 42434	This strike exploits an Arbitrary File Upload vulnerability in Synology Photo Station. The vulnerability is due to improper input validation of user controlled input. A remote, unauthenticated attacker can upload arbitrary files to the target server.
Strike Synology Photo Station PixlrEditorHandler Directory Traversal	CWE: 22 CVE: 2017-11152 EXPLOITDB : 42434	This strike exploits a Directory Traversal vulnerability in Synology Photo Station. The vulnerability is due to improper input validation of the path parameter and incorrect session management. A remote, unauthenticated attacker can write arbitrary files to the target server and log in using a fake authentication mechanism.
Strike ManageEngine ServiceDesk download-file Directory Traversal	CWE: 200 CVE: 2017-11511 BID: 101788	This strike exploits a directory traversal vulnerability in ManageEngine ServiceDesk. HTTP GET requests to the /fosagent/repl/download-file are intended to download files from a specific directory. However, the filepath parameter is not sanitized for directory traversal characters. An attacker can send an HTTP GET request with a specially crafted filepath parameter to download arbitrary files from the target system.
Strike ManageEngine ServiceDesk DownloadSnapshotServlet Directory Traversal	CWE: 22 CVE: 2017-11512 BID: 101789	This strike exploits an absolute path traversal vulnerability in the DownloadSnapshotServlet module on the ManageEngine ServiceDesk application. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation results in the disclosure of arbitrary file contents from the target server.
Strike Microsoft Edge Javascript ParseCatch Type Confusion	CWE: 119 CVE: 2017-11764 BID: 100726	This strike exploits a vulnerability in Microsoft Edge. Specifically, the vulnerability exists within the Chakra engine's ParseCatch function. It is possible to craft javascript in a way that causes type confusion to occur if a catch statement contains an eval function that is encapsulated in a destructuring assignment declaration. This can lead to a memory access violation causing a denial of service in the browser or potentially allowing for remote code execution to occur.
Strike Microsoft Edge Chakra Engine JIT Compiler Incorrect Instruction GenerateBailOut for Patterns	CWE: 119 CVE: 2017-11799 BID: 101126 GOOGLE: 1333 EXPLOITDB : 42998	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to create Javascript in such a way that a change to the opcode of an instruction can generate a bailout but some calling patterns are not considered, and some pointers are not freed or unlinked. This may lead to a denial of service condition in the browser, or potentially remote code execution.

Name	References	Description
Strike Microsoft Edge Chakra Uninitialized Pointers in BoxState Box	CWE: 119 CVE: 2017-11809 GOOGLE: 1338 BID: 101137 EXPLOITDB : 42999	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that uninitialized local variables can be accessed. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge DoBodyLoopStart Out of Bounds Memory Read	CWE: 119 CVE: 2017-11811 BID: 101138	This strike exploits a vulnerability in Microsoft Edge. Specifically, the vulnerability exists within the Chakra engine's DoBodyLoopStart function. When iterating through a loop that contains a switch statement, it is possible to craft javascript in a way that causes an out of bounds memory read. The DoBodyLoopStart function calls compiled code that contains an offset to read a memory address outside the bounds of the allocated dynamic code, which leads to an out-of-bounds memory read.
Strike Microsoft Edge Chakra Engine InlineCallApplyTarget_Shared Incorrect Return	CWE: 119 CVE: 2017-11841 BID: 101733 GOOGLE: 1366 EXPLOITDB : 43181	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to create Javascript in such a way that when a call is made to an Inlinee method the returned method is incorrect and it will potentially skip returning the proper instruction. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Internet Explorer Jscript.dll ArraySlice Uninitialized Variable	CWE: 119 CVE: 2017-11855 BID: 101751 GOOGLE: 1378 EXPLOITDB : 43371	This strike exploits a vulnerability in the Microsoft Internet Explorer browser. Specifically, the vulnerability exists in jscript.dll. It is possible to create an uninitialized type variable when making a call to JsArraySlice. This may lead to a denial of service condition in the browser, or potentially remote code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Edge Chakra Lower Bounds Integer Overflow	CWE: 119 CVE: 2017-11861 BID: 101723 GOOGLE: 1343	This strike exploits a vulnerability in Microsoft Edge. Specifically, the vulnerability exists within the Chakra engine's LowerBoundCheck function. It is possible to craft javascript in such a way, that on a 64bit system, LowerBoundCheck will incorrectly determine whether or not an integer overflow has occurred. When a TypedArray is accessed as a 64bit integer an out of bounds memory access will occur. This can cause a denial of service or potentially lead to remote code execution.
Strike Microsoft Edge Chakra Function Declaration Scope Type Confusion	CWE: 119 CVE: 2017-11870 BID: 101731 GOOGLE: 1367 EXPLOITDB : 43182	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to incorrectly optimize arguments in Javascript, which may cause type confusion to occur. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Internet Explorer Jscript RegExpCompile Buffer Overflow	CWE: 119 CVE: 2017-11890 GOOGLE: 1369 EXPLOITDB : 43369 BID: 102082	This strike exploits a vulnerability in the Microsoft Internet Explorer browser. Specifically, the vulnerability exists in the Javascript engine. It is possible to craft Javascript in such a way that causes a heap overflow when compiling a Regular Expression. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Chakra MinInAnArray MaxInAnArray Type Confusion	CWE: 119 CVE: 2017-11893 BID: 102081 GOOGLE: 1379 EXPLOITDB : 43466	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the javascript Chakra engine. Javascript can be crafted in such a way that allows for type confusion to occur when MinInAnArray or MaxInAnArray methods are called to return the largest or smallest of a series of numbers. The functions fail to properly validate the input and can instead change the type from a JavascriptNativeArray to a VarArray causing type confusion to occur. This may cause a denial of service condition in the browser, or potentially lead to remote code execution.

Name	References	Description
Strike Microsoft Internet Explorer Jscript LastParen Out of Bounds Read	CWE: 200 CVE: 2017-11906 GOOGLE: 1382 EXPLOITDB : 43372 BID: 102078	This strike exploits a vulnerability in the Microsoft Internet Explorer browser. Specifically, the vulnerability exists in the Javascript engine. It is possible to craft Javascript in such a way that causes an out of bounds read in the jscriptRegExpFncObj::LastParen method. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Chakra ASM Out of Bounds Read	CWE: 119 CVE: 2017-11911 BID: 102087 GOOGLE: 1385 EXPLOITDB : 43468	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the javascript Chakra engine. It is possible to create javascript in such a way that an out of bounds read can occur in ASM.js. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Chakra GetPropertyBuiltins scriptFunction Type Confusion	CWE: 119 CVE: 2017-11914 BID: 102088 GOOGLE: 1403 EXPLOITDB : 43713	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the javascript Chakra engine. It is possible to create javascript in such a way that allows for the scriptFunction to be exposed to the user as 'this' when getting the length property. When this happens type confusion occurs. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Chakra JIT Escape Analysis	CWE: 119 CVE: 2017-11918 BID: 102089 GOOGLE: 1396 EXPLOITDB : 43469	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the javascript Chakra engine. It is possible to create javascript in such a way that allows for created variables to escape analysis and get allocated to the stack. This can then allow for the dereference of uninitialized stack values. This may lead to a denial of service condition in the browser, or potentially remote code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cisco License Manager Server ReportCSV Directory Traversal	CWE: 22 CVE: 2017-12263	This strike exploits an information disclosure in Cisco License Manager Server. The vulnerability is due to insufficient validation on user supplied paths when a request is sent to ReportCSV servlet. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target system. Successful exploitation results in the disclosure of the contents of arbitrary files from the target system.
Strike Cisco Prime Network Analysis Module Graph sfile Parameter Directory Traversal	CWE: 20 CVE: 2017-12285 BID: 101527	This strike exploits a directory traversal vulnerability in Cisco Prime Network Analysis Module. The sfile parameter of HTTP requests to /capture/graph.php is intended to read and delete a specified graph file. It is not sanitized for directory traversal characters. An attacker can send specially crafted HTTP requests to delete arbitrary files.
Strike HPE Intelligent Management Center saveSelectedDevices Expression Language Injection	CWE: 20 CVE: 2017-12491 BID: 100367	This strike exploits An Expression Language injection vulnerability in Hewlett Packard Enterprise (HPE) Intelligent Management Center. The vulnerability is due to improper input validation of HTTP POST request payload. A remote, authenticated attacker can execute arbitrary code on the targeted system by sending a crafted HTTP request to the target server.
Strike HPE Intelligent Management Center ictExpertDownload beanName Expression Language Injection	CWE: 20 CVE: 2017-12500 BID: 100367	This strike exploits An Expression Language injection vulnerability in Hewlett Packard Enterprise (HPE) Intelligent Management Center. The vulnerability is due to improper input validation of HTTP request parameters. A remote, authenticated attacker can execute arbitrary code on the targeted system by sending a crafted HTTP request to the target server.
Strike HPE Intelligent Management Center userSelectPagingContent beanName Expression Language Injection	CWE: 20 CVE: 2017-12521 BID: 100367	This strike exploits an Expression Language Injection vulnerability in Hewlett Packard Enterprise (HPE) Intelligent Management Center. The vulnerability is due to improper input validation of HTTP request parameters. A remote, authenticated attacker can execute arbitrary code on the targeted system by sending a crafted HTTP request to the target server.
Strike HPE Intelligent Management Center wmiConfigContent beanName Expression Language Injection	CWE: 20 CVE: 2017-12526 BID: 100367	This strike exploits An Expression Language injection vulnerability in Hewlett Packard Enterprise (HPE) Intelligent Management Center. The vulnerability is due to improper input validation of the beanName HTTP request parameter. A remote, authenticated attacker can execute arbitrary code on the targeted system by sending a crafted HTTP request to the target server.
Strike HPE iLO 4 1.00-2.50 Administrator Account Creation	CVE: 2017-12542 BID: 100467	This strike exploits an authentication bypass vulnerability in HPE Integrated Lights-out (iLO 4). This vulnerability is due to inadequate input filtering in the HTTP Connection header. The vulnerability could be exploited remotely by creating an administrator account and then execution of code.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike HPE System Management Homepage gsearch.php.en Cross-Site Scripting (XSS)	CWE: 79 CVE: 2017-12544 BID: 101029	This strike exploits a cross-site scripting vulnerability in HPE System Management Homepage. This vulnerability is due to inadequate input filtering in "prod" field. By exploiting this vulnerability an attacker could cause arbitrary scripting code to be executed by the target user's browser.
Strike HPE intelligent Management Center WebDMDebugServlet Remote Code Execution	CWE: 502 CVE: 2017-12557 BID: 101152 EXPLOITDB : 45952	An insecure deserialization vulnerability exists in HPE intelligent Management Center PLAT v7.3 E0504. The flaw arises due to lack of security checks when processing the POST payload for the '/imc/topo/WebDMDebugServlet' endpoint. Successful attacks result in arbitrary remote code execution with root privileges.
Strike HPE Intelligent Management Center imcweb_dm.jar Remote Code Execution	CWE: 502 CVE: 2017-12558 BID: 101152	This strike exploits a remote code execution vulnerability in Hewlett Packard Enterprise (HPE) Intelligent Management Center. The vulnerability is due to insecure deserialization of user input data sent through HTTP. A remote, unauthenticated attacker can run arbitrary commands on the targeted system by sending a crafted HTTP request to the target server.
Strike Apache Struts2 Freemarker Tag Code Execution	CWE: 20 CVE: 2017-12611 BID: 100829	This strike exploits a remote code execution vulnerability in Apache Struts2. When using an unintentional expression in Freemarker tag instead of string literals, it is possible for an attacker to craft a malicious payload that may allow for remote code execution to occur.
Strike Apache Tomcat JSP Upload Remote Code Execution	CWE: 434 CVE: 2017-12615 BID: 100901	This strike exploits a remote command execution vulnerability in Apache Tomcat. The vulnerability allows attackers to upload arbitrary files to the Tomcat application server by utilizing the HTTP PUT method. By uploading a .JSP file to the Tomcat Application Server, an attacker can execute malicious code on the remote machine.
Strike Apache Tomcat Misconfigured HTTP PUT Remote Code Execution	CWE: 434 CVE: 2017-12617	This strike exploits a file upload vulnerability in Apache Tomcat. The vulnerability arises from a misconfiguration in handling PUT requests. When Tomcat is configured with readonly set to false and PUT requests are allowed, attackers can upload files with names ending in ".jsp///". Tomcat removes the trailing slashes, saving the file as a ".jsp" that includes attacker-controlled data. A remote, unauthenticated attacker can exploit this vulnerability by sending a PUT request with a malicious payload in the .jsp file, which executes when accessed. Successful exploitation could result in remote code execution within the context of the user running the Apache Tomcat.

Name	References	Description
Strike Apache Solr RunExecutableListener Code Execution	CWE: 611 CVE: 2017-12629 BID: 101261 EXPLOITDB : 43009	This strike exploits a remote code execution in Apache Solr. The vulnerability exists due to Apache Solr RunExecutableListener class can be used to execute arbitrary commands on postCommit or newSearcher events. Successful exploitation will result in code execution.
Strike Apache Solr Xmlparser XXE Expansion	CWE: 611 CVE: 2017-12629 BID: 101261 EXPLOITDB : 43009	This strike exploits an XML External Entity expansion vulnerability in Apache Solr. The vulnerability exists due to insufficient checking when handling the incoming XML external entities. Successful exploitation will result in code execution.
Strike Apache CouchDB Remote Privilege Escalation	CWE: 269 CVE: 2017-12635 BID: 101868	This strike exploits a remote privilege escalation vulnerability in Apache CouchDB. The vulnerability is due to insufficient validation of user-supplied JSON objects. Successful exploitation will allow an attacker to create an administrative account within CouchDB.
Strike Apache CouchDB Remote Code Execution	CWE: 78 CVE: 2017-12636	This strike exploits a remote code execution vulnerability in Apache CouchDB. CouchDB administrative users can configure the database server via HTTP. Some of the configuration options include paths for operating system-level binaries that are subsequently launched by CouchDB. Successful exploitation will allow a CouchDB admin user to execute arbitrary shell commands as the CouchDB user.
Strike Cacti spikekill php Cross-Site Scripting	CWE: 79 CVE: 2017-12927	This strike exploits a reflected cross-site scripting vulnerability in Cacti. This vulnerability is due to improper validation of the method parameter within spikekill.php. The method value should be one of the stddev, float, variance, or fill. A remote attacker could exploit this vulnerability by enticing an authenticated user to visit a maliciously crafted URL in which the value of method is not one of the previously mentioned values. Successful exploitation could lead to arbitrary script code execution in the context of the user's browser.
Strike TP-Link WiFi router Authenticated PingIframeRpm Stack Buffer Overflow	CWE: 119 CVE: 2017-13772 EXPLOITDB : 43022	This strike exhibits the network behavior of a buffer overflow vulnerability inside TP-Link WiFi router. The vulnerability is due do insufficient user input validation passed to 'ping_addr' parameter pertaining to 'PingIframeRpm.htm' form. By crafting a malicious HTTP request, an attacker can cause DoS conditions or achieve code execution on the target device.

Name	References	Description
Strike Apple Safari WebKit WebCore FormSubmission create Use After Free	CWE: 119 CVE: 2017-13791 GOOGLE: 1355	This strike exploits a vulnerability in Apple Safari WebKit. Specifically the vulnerability exists in WebKit's WebCore::FormSubmission::create method. An attacker can craft javascript in such a way that when invoking the create method in a form a use after free condition can occur. This can lead to a denial of service or potentially allow for remote code execution on the vulnerable system.
Strike Apple Safari WebKit WebCore RenderObject previousSibling Use After Free	CWE: 119 CVE: 2017-13798 GOOGLE: 1354	This strike exploits a vulnerability in Apple Safari WebKit. Specifically the vulnerability exists in WebKit's WebCore::RenderObject::previousSibling method. An attacker can craft javascript in such a way that when invoking the create method in a form a use after free condition can occur. This can lead to a denial of service or potentially allow for remote code execution on the vulnerable system.
Strike Trend Micro Mobile Security Enterprise slink_id SQL injection	CWE: 89 CVE: 2017-14078 BID: 100966	This strike exploits a SQL injection vulnerability in Trend Micro Mobile Security Enterprise. The slink_id HTTP parameter is vulnerable to SQL injection. slink_id can also be accessed via JSON in the HTTP request body. An attacker can send a specially crafted HTTP request to achieve SQL injection. Successful exploitation may lead to arbitrary SQL code execution with SYSTEM privileges.
Strike Dell EMC Storage Manager Server Directory Traversal	BID: 103467 CWE: 22 CVE: 2017-14384	The vulnerability allows attackers read access to arbitrary file contents accessible in the Dell EMC Storage Manager server by insufficient validation of user input on requests. Successful exploitation could result in arbitrary file accessible on target with SYSTEM privileges.
Strike NetIQ Access Manager Identity Server Directory Traversal	CVE: 2017-14803 BID: 100901	The vulnerability allows attackers read access to arbitrary file contents accessible in the Micro Focus NetIQ Access Manager server by insufficient validation of user input on requests sent to the OspUIBasicSSODownload servlet.
Strike Bacula-Web job.php GET request SQL Injection	CWE: 89 CVE: 2017-15367	An SQL injection vulnerability exists in Bacula Web appliance. The vulnerability is due to insufficient user-supplied input validation within job.php script. The successful exploitation of this vulnerability can result in database information disclosure without authentication via a specially crafted HTTP GET request.
Strike Apache httpd FilesMatch Policy Bypass	CWE: 20 CVE: 2017-15715 BID: 103525	This strike exploits a policy bypass vulnerability in Apache httpd FilesMatch. FilesMatch is intended to prevent files which do not match certain regex patterns to be uploaded via HTTP PUT messages. One of these patterns is AP_REG_DOLLAR_ENDONLY, which is intended to prevent files ending with the character. However, this option does not work properly, allowing for files ending with to be uploaded. An attacker can send a specially crafted HTTP PUT message to bypass the policy and upload arbitrary files.

Name	References	Description
Strike Palo Alto Networks Management Interface Authentication Bypass	CVE: 2017-15944 EXPLOITDB : 43342 BID: 102079	This strike exploits a management interface authentication bypass vulnerability in Palo Alto Networks PAN-OS 6.1.18 and earlier, PAN-OS 7.0.18 and earlier, and PAN-OS 7.1.13 and earlier. Note: A remote user can exploit a combination of vulnerabilities in the management interface to execute arbitrary commands on the target system. The code will run with root privileges. This strike simulates panAuthCheck authentication bypass.
Strike NetGain Systems Enterprise Manager settings.upload filename Directory Traversal	CWE: 668 CVE: 2017-16603 BID: 102307	This strike exploits a vulnerability in NetGain Systems Enterprise Manager prior to v7.2.766. The vulnerability is caused by insufficient validation of user input in http requests. Successful exploitation could result in arbitrary file accessible on target server.
Strike Roundcube Webmail timezone File Disclosure Vulnerability	CWE: 552 CVE: 2017-16651	This strike exploits Local File Inclusion vulnerability in Roundcube webmail. The vulnerability occurs due insufficient input validation in conjunction with the file-based attachment plugins. An authenticated remote attacker with an active session can exploit this vulnerability by sending crafted request to the server. Successful exploitation of this vulnerability leads to information disclosure by accessing arbitrary files
Strike Advantech WebAccess SCADA gmicons.asp Arbitrary File Upload	CWE: 434 CVE: 2017-16736	An arbitrary file overwrite vulnerability has been identified in Advantech WebAccess SCADA web platform. The vulnerability is caused by the lack of proper input sanitisation of the gmicons.asp picfile parameter. The vulnerability can be exploited by sending a specially-crafted request, allowing the attacker to execute code on the remote machine with the privileges of the application process.
Strike Huawei HG532 Router Remote Command Execution	CWE: 20 CVE: 2017-17215 BID: 102344	This strike exploits a remote command execution vulnerability in Huawei HG532 Router. The vulnerability is due to insufficient validation of NewDownloadURL and NewStatusURL in SOAP XML. The exploit has been used in okiru/satori, a variant of Mirai.
Strike Ruby Net FTP Command Injection	CWE: 78 CVE: 2017-17405 BID: 102204 EXPLOITDB : 43381	This strike exploits a remote command injection vulnerability in Ruby before 2.4.3. The vulnerability is due to ruby NET::FTP, which will execute any command after the " " pipe character in the localfile argument. This vulnerability could allow an unauthorized user to execute arbitrary code on the server.

Name	References	Description
Strike Quest NetVault Backup NVBUEventHistory SQL Injection	CWE: 89 CVE: 2017-17412 BID: 102252	An SQL injection vulnerability exists in Quest NetVault Backup appliance. The vulnerability is due to insufficient user-supplied input validation within Server Process Manager Service. The successful exploitation of this vulnerability can result in database information disclosure without authentication via a specially crafted HTTP request.
Strike Quest NetVault Backup NVBUTransferHistory SQL Injection	CWE: 89 CVE: 2017-17419	An SQL injection vulnerability exists in Quest NetVault Backup appliance. The vulnerability is due to insufficient user-supplied input validation within Server Process Manager Service. The successful exploitation of this vulnerability can result in database information disclosure without authentication via a specially crafted HTTP GET request.
Strike Quest NetVault Backup NVBUJobCountHistory SQL Injection	CWE: 89 CVE: 2017-17420 BID: 102252	An SQL injection vulnerability exists in Quest NetVault Backup appliance. The vulnerability is due to insufficient user-supplied input validation within Server Process Manager Service. The successful exploitation of this vulnerability can result in database information disclosure without authentication via a specially crafted HTTP request.
Strike EmbedThis GoAhead Web Server Code Execution	CWE: 20 CVE: 2017-17562	This strike exploits a remote code execution vulnerability in EmbedThis GoAhead Web Server. The vulnerability is due to insufficient validation of CGI variables. To exploit the vulnerability, an attacker would create a HTTP CGI request that uses sets LD_PRELOAD=/proc/self/fd/0 in the query string and sets the POST data of the request to be in the form of a malicious shared library for the architecture of the device.
Strike Zyxel P660HN-T1A Routers Command Injection Vulnerability	CVE: 2017-18368 CWE: 78	This strike exploits an OS command injection vulnerability in Zyxel P660HN-T1A Routers. The vulnerability is due to the improper neutralization of special elements in the parameter "remote_host". An unauthenticated attacker could exploit this vulnerability by executing some OS commands by sending a crafted HTTP request and might result in remote code execution.
Strike MacOS HelpViewer x-help-script XSS Path Traversal and Local File Read	CWE: 79 CVE: 2017-2361 GOOGLE: 1040 BID: 95723	This strike exploits a vulnerability in MacOS HelpViewer. Specifically, HelpViewer's WebView has a protocol handler x-help-script, that can be used to access a local file via path traversal. An attacker can craft javascript that will allow for an XMLHttpRequest to open this local file. This strike demonstrates this by opening one of the following apps, Calculator, Messages, Preview, or Notes, by accessing this HTML on a remote server with a vulnerable version of MacOS.

Name	References	Description
Strike Adobe Flash ATF Thumbnailing Heap Overflow	CWE: 119 CVE: 2017-2933 GOOGLE: 1015 BID: 95347	This strike exploits a remote code execution vulnerability in Adobe Flash Player. The vulnerability is due to a heap overflow related to texture compression. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in abnormal termination of the flash process.
Strike Adobe Flash ATF Planar Decompression Heap Overflow	CWE: 119 CVE: 2017-2934 GOOGLE: 1016 BID: 95347	This strike exploits a remote code execution vulnerability in Adobe Flash Player. The vulnerability is due to a heap overflow in planar block decompression. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in abnormal termination of the flash process.
Strike Adobe Flash AVC Header Slicing Heap Overflow	CWE: 119 CVE: 2017-2935 GOOGLE: 1017 BID: 95347	This strike exploits a remote code execution vulnerability in Adobe Flash Player. The vulnerability is due to a heap overflow in AVC header slicing. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in abnormal termination of the flash process.
Strike Adobe Flash FLV YUVPlane Decoding Heap Overflow	CWE: 119 CVE: 2017-2986 GOOGLE: 1008 BID: 96193	This strike exploits a remote code execution vulnerability in Adobe Flash Player. The vulnerability is due to an heap overflow in YUVPlane decoding. An attacker can entice a target to open a specially crafted flash file to trigger the vulnerability. Successful exploitation may result in abnormal termination of the flash process.
Strike Oracle Fusion Middleware MapViewer Code Execution	CVE: 2017-3230 BID: 97746	This strike exploits a Code Execution vulnerability in the Oracle Fusion Middleware MapViewer component of Oracle Fusion Middleware. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data.
Strike Oracle WebLogic Server OS Command Injection Vulnerability	CWE: 78 CVE: 2017-3506	This strike exploits an OS command injection vulnerability in Oracle WebLogic Server. The vulnerability is caused by insecure deserialization of untrusted data. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted serialized object to the vulnerable WebLogic Server. When the server processes this object, it deserializes the data, leading to the execution of the attacker's code.

Name	References	Description
Strike Spring Web Flow SPEL Command Injection	CWE: 1188 CVE: 2017-4971 BID: 98785	This strike exploits a remote command injection vulnerability in the Pivotal Spring Web Flow framework. The vulnerability exists due to insufficient validation of binding SPEL expression. The vulnerability can be exploited by sending a specially crafted HTTP request, allowing arbitrary command injection.
Strike Google Chrome Javascript V8 Array.indexOf Information Leak	CWE: 200 CVE: 2017-5040 BID: 96767 GOOGLE: 691323	This strike exploits a vulnerability in the Google Chrome Browser. Specifically, the vulnerability exists in the Javascript V8 engine. It is possible to craft Javascript in such a way that when calling Array.indexOf, properties of the array can be changed, and certain values in memory can be disclosed to the user.
Strike Google Chrome Javascript V8 Out of Bounds Read	CWE: 125 CVE: 2017-5053 GOOGLE: 702058 BID: 97220	This strike exploits a vulnerability in the Google Chrome Browser. Specifically, the vulnerability exists in the Javascript V8 engine. It is possible to craft Javascript in such a way that an out of bounds read of memory can occur. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Google Chrome Javascript Crankshaft Type Confusion	CWE: 704 CVE: 2017-5070 BID: 98861	This strike exploits a vulnerability in Google Chrome. Specifically, the vulnerability exists within Chrome's javascript engine V8. When javascript is encountered, the V8 engine sends the code to Crankshaft to be optimized. It is here where the vulnerability is found when validating two pointers. One pointer may point to a constant, and the other may point to a different unexpected object type. Further processing of this code can lead to type confusion. This will cause a denial of service in the browser, and can potentially lead to remote code execution.
Strike Google Chrome Javascript V8 Engine FindSharedFunction Info Out of Bounds Read	CWE: 125 CVE: 2017-5071 GOOGLE: 715582 BID: 98861	This strike exploits a vulnerability in the Google Chrome Browser. Specifically, the vulnerability exists in the Javascript V8 engine. It is possible to craft Javascript in such a way that an out of bounds read will occur in FindSharedFunctionInfo. This may lead to a denial of service condition in the browser, or potentially remote code execution.

Name	References	Description
Strike Google Chrome WebGL2 ReadPixels Buffer Overflow	CWE: 119 CVE: 2017-5112 BID: 100610 GOOGLE: 740603	This strike exploits a vulnerability in Google Chrome. Specifically, the vulnerability exists within the WebGL2 library's ReadPixels function. It is possible to craft javascript in such a way that when the rows of pixel data of a webgl2 canvas are read and copied to an offset with the PACK_SKIP_ROWS parameter, a heap buffer overflow can occur. This can cause a denial of service or potentially lead to remote code execution.
Strike Advantech WebAccess Template.aspx SQL Injection	CWE: 89 CVE: 2017-5154 BID: 95410	This strike exploits a SQL injection in Advantech WebAccess 8.1. The vulnerability is due to improper sanitization of user supplied input in template parameter. By exploiting this vulnerability, an authenticated attacker can execute arbitrary SQL queries on the server.
Strike PHPMailer Local Information Disclosure	CWE: 200 CVE: 2017-5223 BID: 95328 EXPLOITDB : 43056	This strike exploits a local information disclosure vulnerability in PHPMailer. The vulnerability is due to insufficient validation of user-supplied input by the msgHTML function. Successful exploitation will allow an attacker to obtain sensitive information on the server.
Strike Mozilla Firefox Table Use-After-Free	BID: 96664 CWE: 416 CVE: 2017-5404 GOOGLE: 1130	This strike exploits a remote code execution vulnerability in Mozilla Firefox. The vulnerability can be triggered by manipulating range elements within selections. Successful exploitation of this vulnerability could result in the execution of arbitrary code on the target system.
Strike Mozilla Firefox http-index-format File Buffer Overflow	CWE: 119 CVE: 2017-5444 BID: 97940	This strike exploits a buffer overflow vulnerability in Mozilla Firefox. When parsing content-type application/http-index-format data, it is possible for an out of bounds read of memory to occur causing a buffer overflow. This can cause a denial of service condition in the browser or potentially allow for remote code execution to occur.
Strike Apache Struts2 OGNL Command Execution	BID: 96729 CWE: 20 CVE: 2017-5638	This strike exploits a remote command execution vulnerability in Apache Struts. An HTTP request with a specially crafted content-type can be used to execute arbitrary commands. Successful exploitation may result in command execution.

Name	References	Description
Strike Intel AMT Remote PRivilege Escalation Vulnerability	CVE: 2017-5689 BID: 1038385	This strike exploits a privilege escalation vulnerability in Intel Active Management Technology. The vulnerability is due to improper input validation when checking parameters in the Authorization HTTP request header. An unprivileged attacker can gain system privileges of AMT by sending an HTTP Digest authentication request with an empty response parameter.
Strike Spectre Attack (Variant 1 Bounds Check Bypass) - Browser Memory Leak through Javascript Engine	CWE: 200 CVE: 2017-5753 BID: 102371	This strike exploits the Spectre vulnerability identified in modern Intel CPUs by leveraging a side-channel attack through the Javascript engine within a browser. This vulnerability is due to incomplete clearance of CPU cache memory after invalidation of a speculative execution result. By exploiting this vulnerability, an attacker can obtain sensitive data, like stored passwords or session IDs, from the browser's process memory.
Strike HPE Intelligent Management Center UrlAccessController Authentication Bypass	CWE: 287 CVE: 2017-5791	This strike exploits an authentication bypass vulnerability in HPE Intelligent Management Center. This vulnerability is due to doFilter method which contains multiple ways to bypass authentication if the URI contains specific strings. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target system. Successful exploitation allows to bypass authentication requirements, which can be leveraged to execute arbitrary code in the context of SYSTEM.
Strike HPE Intelligent Management Center Remote Unauthenticated filePath parameter Information Disclosure	CWE: 200 CVE: 2017-5797 BID: 97214	This strike exploits an information disclosure vulnerability in Hewlett Packard Enterprise (HPE) Intelligent Management Center (IMC). Specifically, an authentication check is not made when processing HTTP requests sent to the URI / servicedesk/servicedesk/fileDownload. An unauthenticated attacker can specify a file and path as the value of the filePath parameter to disclose contents on the remote machine.
Strike HPE Network Automation RedirectServlet SQL Injection	CWE: 89 CVE: 2017-5810 BID: 98331	This strike exploits an SQL injection vulnerability in HPE Network Automation. The RedirectServlet constructs SQL queries in order to retrieve information from the database, and does not allow specific characters to be passed in these parameters. However, a malicious attacker can construct a query using the deviceID parameter that will perform an SQL UNION and return an encryption key from the database in the primaryIPAddress parameter. When combined with the authentication bypass this attack can lead to SQL command execution in the remote database.
Strike HPE Network Automation FileServlet Information Disclosure	CWE: 200 CVE: 2017-5811 BID: 98331	This strike exploits an information disclosure vulnerability in HPE Network Automation. Specifically the FileServlet class fails to properly validate the encrypted file path provided by the user. A malicious attacker can craft a request via the tk parameter that will allow for file contents to be disclosed. This attack can be combined with an SQL injection (CVE-2017-5810) to provide the key used for encryption and decryption

Name	References	Description
Strike HPE Network Automation PermissionFilter Authentication Bypass	CWE: 89 CVE: 2017-5812 BID: 98331	This strike exploits an authentication bypass vulnerability in HPE Network Automation. The PermissionFilter class performs a check to determine if a URI request requires authentication. However, if traversal characters are used in conjunction with these strings an attacker can bypass authentication to allow access to the requested page.
Strike NetGear DGN2200 Devices ping.cgi Remote Code Execution	CVE: 2017-6077 CWE: 78	This strike exploits an command injection vulnerability in NetGear DGN2200 Devices. The vulnerability is due to improper input validation of parameters used in ping.cgi component on NetGear DGN2200 devices. A remote, authenticated attacker could exploit this vulnerability by sending a crafted HTTP request and might result in remote code execution in the context of running service.
Strike D-Link Directory Traversal Information Disclosure	CWE: 22 CVE: 2017-6190 EXPLOITDB : 41840 BID: 97620	This strike exploits a directory traversal vulnerability present in multiple firmware versions of D-Link routers. The vulnerability can be exploited by performing GET requests under the path '/uir' of router's web interface. By exploiting it, an attacker may read arbitrary files from the filesystem which could lead further to credentials disclosure.
Strike Symantec Messaging Gateway performRestore Command Injection	CWE: 20 CVE: 2017-6327	This strike exploits a command injection vulnerability in Symantec Messaging Gateway. The vulnerability is due to authentication bypass in the 'LoginAction' and improper validation of input passed to 'performRestore' method. Specifically, the 'localBackupFileSelection' parameter is not properly sanitized. The flaw may be exploited by an unauthenticated attacker to execute arbitrary code in the context of the root user.
Strike NETGEAR DGN2200 Devices OS Command Injection Vulnerability	CVE: 2017-6334 CWE: 78	This strike exploits an OS command injection vulnerability on NETGEAR DGN2200 routers. The vulnerability is due improper input validation in user-supplied input , allowing shell metacharacters in the host_name field of an HTTP POST request in dnslookup.cgi script. A remote authenticated attacker can exploit this by sending a crafted POST request with valid login details. Successful exploitation could allow the attacker to execute arbitrary OS commands on the device.
Strike Cisco Prime Collaboration Provisioning ScriptMgr BeanShell Authentication Bypass	CWE: 862 CVE: 2017-6622 BID: 98520	This strike exploits an authentication bypass vulnerability in Cisco Prime Collaboration Provisioning ScriptMgr servlet. The ScriptMgr servlet is intended to allow authenticated users to access BeanShell, which can execute Java and Javascript code with root privileges. However, it only authenticates HTTP GET and POST requests. Other HTTP requests, such as HEAD, are processed without authentication. An attacker can send an HTTP request other than GET or POST to the vulnerable servlet to achieve execution of arbitrary Java or Javascript code with root privileges.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Zyxel EMG2926 diagnostic tools OS Command Injection	CWE: 78  CVE: 2017-6884  EXPLOITDB : 41782	This strike exploits a command injection vulnerability in Zyxel EMG2926 home router. The vulnerability is due to improper validation of input passed to 'nslookup' function located in the diagnostic tools. By exploiting this vulnerability, a remote unauthenticated attacker can execute arbitrary OS commands on the target router.
Strike Horde Webmail OS Command Injection	CWE: 78  CVE: 2017-7413	The strike exploits an OS command injection vulnerability in Horde Groupware Webmail client. The vulnerability originates from the lack of sanitization in handling the 'generate_email' parameter when generating PGP keys. The parameter will be later passed as a command line argument to the 'gpg' binary, allowing arbitrary commands execution on the host system.
Strike MXview Industrial Network Management Software Information Disclosure	CWE: 200  CVE: 2017-7455  EXPLOITDB : 41850	This strike exploits an information disclosure vulnerability in MXview Industrial Network Management Software. The vulnerability is due to lack of access controls and improper handling of HTTP requests. Successful exploitation will allow an attacker to obtain sensitive information from the server, including SSL private key.
Strike Mantis Bug Tracker Password Reset Vulnerability	CWE: 640  CVE: 2017-7615  BID: 97707	This strike exploits a remote password reset vulnerability in Mantis Bug Tracker. The vulnerability is due to improper input validation when checking password reset requests. A remote attacker can reset the password via an empty confirm_hash value to verify.php.
Strike Apache HTTP Server Token Out of Bounds Read	CWE: 20  CVE: 2017-7668  BID: 99137	This strike exploits a denial of service vulnerability in Apache HTTP Server. The vulnerability is due to an out-of-bounds that read exists in Apache when handling HTTP request with a malicious connection header field. By maliciously crafting a sequence of request headers, an attacker may be able to cause a DoS attack.
Strike PHP gdImageCreateFrom GifCtx Out Of Bound Read	CWE: 200  CVE: 2017-7890  BID: 99492	This strike exploits a PHP information disclosure vulnerability before version 5.6.31 and 7.x before 7.1.7 . This vulnerability is due to improper handling of objects in memory under GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c file. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted image file to the target server. Successful exploitation results in information disclosure.
Strike Schneider Umotion Builder localize SQL Injection	CWE: 89  CVE: 2017-7973  BID: 99344	This strike exploits a SQL injection in Schneider Electric U.motion Builder. The vulnerability is due to improper sanitization of user supplied input in username parameter. By exploiting this vulnerability, an attacker can execute arbitrary SQL queries on the server.

Name	References	Description
Strike Schneider Umotion Builder Runscript Path Traversal	CWE: 22 CVE: 2017-7974 BID: 99344	This strike exploits a Path Traversal vulnerability in Schneider Electric U.motion Builder. The vulnerability is due to improper sanitization of user supplied input in s parameter. By exploiting this vulnerability, an attacker can read sensitive information on the server.
Strike Exponent CMS eaasController php api Function SQL Injection	CWE: 89 CVE: 2017-7991	This strike exploits an SQL injection vulnerability in Exponent CMS. The vulnerability is due to a lack of input validation on the apikey HTTP parameter by the api() function. A remote, unauthenticated user can exploit this vulnerability by sending a crafted HTTP request to the affected page. Successful exploitation could result in the execution of arbitrary SQL commands on the target server.
Strike EMC Data Protection Advisor Application Service Static Credentials Authentication Bypass	CWE: 798 CVE: 2017-8013	This strike exploits a static credentials authentication bypass vulnerability in the EMC Data Protection Advisor Application service. This vulnerability is due to hard-coded hidden user entries within the application database. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted request with one of the undocumented credentials in the Authorization header. Successful exploitation would allow attacker to bypass authentication under the context of the Administrator.
Strike Microsoft Edge AsmJsInterpreter Method Use After Free	CWE: 119 CVE: 2017-8603 BID: 99406	This strike exploits a use after free vulnerability in the Microsoft Edge Browser. Specifically, the vulnerability exists in the AsmJsInterpreter method in the Javascript Chakra engine in Microsoft Edge. When creating an asm function with a template literal an object that gets created and freed is later referenced, triggering a use after free condition. An attacker could craft code in such a way that would cause a denial of service condition in the browser or potentially allow for remote code execution to occur.
Strike Microsoft Edge Chakra Uninitialized Arguments	CWE: 119 CVE: 2017-8640 BID: 100051 GOOGLE: 1297 EXPLOITDB : 42476	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. Javascript can be crafted in such a way that allows for the function argument object to be uninitialized. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Chakra Javascript Engine EvalHelper Argument Length Integer Overflow	CWE: 119 CVE: 2017-8641 BID: 100057 EXPLOITDB : 42465	This strike exploits an Integer Overflow vulnerability in the Microsoft Edge Browser. Specifically, the vulnerability exists when the eval method is called with an overly large string value as the argument. An attacker could craft code in such a way that would cause a denial of service condition in the browser or potentially allow for remote code execution to occur.

Name	References	Description
Strike Microsoft Edge Chakra ProcessLinkFailedAsmJsModule Incorrect Reparse	CWE: 119 CVE: 2017-8645 BID: 100052 GOOGLE: 1271 EXPLOITDB : 42469	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. If the Javascript engine cannot link the asmjs module it gets treated as a normal function, however, when this code is reparsed certain cases are not correctly handled, which can result in binding incorrect information to the constructor. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Destructuring Assignment Argument Uninitialized Variable Use	CWE: 119 CVE: 2017-8656 BID: 100033 EXPLOITDB : 42464 GOOGLE: 1266	This strike exploits a vulnerability in Microsoft Edge's Javascript Chakra engine. Specifically, there exists a case where a destructuring assignment is passed as an argument to the catch statement, and the variable inside does not get properly initialized. This use of uninitialized memory when the variable is referenced later may result in a denial of service in the browser or potentially lead to remote code execution.
Strike Microsoft Edge Chakra Uninitialized arguments Object	CWE: 119 CVE: 2017-8670 BID: 100070 GOOGLE: 1298 EXPLOITDB : 42477	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the javascript Chakra engine. Javascript can be crafted in such a way that allows for the function argument object to be uninitialized. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Chakra Engine JavascriptFunction EntryCall Mishandles CallInfo	CWE: 119 CVE: 2017-8671 BID: 100071 EXPLOITDB : 42475 GOOGLE: 1295	This strike exploits a vulnerability in Microsoft Edge's Javascript Chakra engine. The Chakra engine uses the args.Info.Count - 1 as the length of the arguments when given. So this value must be 1 or greater. However, a condition exists in the Chakra Javascript engine where the args.Info.Count can be decremented to 0. This may result in a denial of service in the browser or potentially lead to remote code execution.

Name	References	Description
Strike Microsoft Edge Chakra ConvertObjectToObjectPattern Type Confusion	BID: 100733  CWE: 119  CVE: 2017-8729  GOOGLE: 1308  EXPLOITDB : 42763	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that the ConvertObjectToObjectPattern method will contain incorrect members. When one of these members is referenced type confusion will occur. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge COptionsCollectionCacheItem Out of Bounds Memory Read	CWE: 119  CVE: 2017-8734  BID: 100738  EXPLOITDB : 42759	This strike exploits a vulnerability in Microsoft Edge. Specifically, the vulnerability exists within edgehtml's COptionsCollectionCacheItem::GetAt function. When parsing html textarea, select, and optgroup elements, it is possible to create an out of bounds read condition that allows for the reading of heap buffer memory. This can cause a denial of service or potentially lead to remote code execution.
Strike Microsoft Edge Chakra Object.setPrototypeOf Of Memory Corruption	CWE: 119  CVE: 2017-8751  GOOGLE: 1339  EXPLOITDB : 43151	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. Javascript can be crafted in such a way that allows for memory corruption to occur when a call to setPrototypeOf is made. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Joomla com_fields SQL Injection	CWE: 89  CVE: 2017-8917  BID: 98515  EXPLOITDB : 42033	This strike exploits an SQL injection vulnerability in Joomla! 3.7. The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure, database corruption, denial of service and others.
Strike HPE Intelligent Management Center flexFileUpload Arbitrary File Upload	CWE: 22  CVE: 2017-8961	This strike exploits an arbitrary file upload vulnerability in Hewlett Packard Enterprise (HPE) Intelligent Management Center. By design, the uri /imc/flexFileUpload should accept xml documents in multipart/form-data encoding. However, file extension and type are not validated, allowing for arbitrary file upload. An attacker can send specially crafted HTTP POST requests containing an arbitrary file with multipart/form-data to upload the file. If the file is of type .jsp or .jspx, the attacker can then request the file to achieve arbitrary code execution with SYSTEM privileges.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike HPE Intelligent Management Center perfAccessMgrServl et Insecure Java Deserialization	CWE: 502 CVE: 2017-8962	This strike exploits an insecure java deserialization in Hewlett Packard Enterprise (HPE) Intelligent Management Center (IMC). This vulnerability is due to improper validation of Java serialized objects before deserialization . An attacker could send a specially crafted HTTP POST request to achieve arbitrary command execution with either SYSTEM or root privileges.
Strike HPE Moonshot Provisioning Manager Appliance Directory Traversal	CWE: 20 CVE: 2017-8977	This strike exploits a directory traversal vulnerability in the HPE Moonshot Provisioning Manager Appliance. The vulnerability is due to inadequate authentication and input validation in the server_response.py script. A remote, unauthenticated attacker can exploit this vulnerability by sending requests with crafted filenames containing directory traversal patterns. Successful exploitation enables attackers to overwrite arbitrary files accessible to the web application, potentially leading to a denial-of-service condition.
Strike Apache httpd mod_auth_digest Memory Access Denial of Service	CWE: 200 CVE: 2017-9788	This strike exploits a memory access error in Apache httpd. The value placeholder in Proxy-Authorization or Authorization headers of type 'Digest' is not initialized or reset by mod_auth_digest. A remote, unauthenticated attacker could exploit this vulnerability by sending an initial key with no '=' assignment which could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.
Strike Apache Struts2 Plugin OGNL Command Execution	CWE: 20 CVE: 2017-9791 BID: 99484	This strike exploits a remote command execution vulnerability in the Struts 1 plugin in Apache Struts 2.3.x. When using the Struts 1 plugin in Struts 2, and the Struts 1 action and value are part of a message presented to the user, it is possible for an attacker to craft a malicious field value that may allow for remote code execution to occur.
Strike Apache Struts2 REST Plugin XStream DoS	CWE: 20 CVE: 2017-9793 BID: 100611	This strike exploits a denial of service vulnerability in Apache Struts2 REST plugin. Attacker can send a crafted XML file to cause the application server to terminate. Apache Struts 2.3.7 through 2.3.33, and 2.5 through 2.5.12 are vulnerable.
Strike Apache Struts REST plugin with XStream handler Command Execution	CWE: 502 CVE: 2017-9805 BID: 100609	This strike exploits a remote command execution vulnerability in Apache Struts. The vulnerability is due to insecure deserialization of data by XStreamHandler in Apache Struts REST Plugin. Successful exploitation may result in executing arbitrary code on the target system.
Strike PHPUnit Command Injection	CWE: 94 CVE: 2017-9841	This strike exploits a command injection vulnerability in PHPUnit. This vulnerability lies within the /phpunit/src/Util/PHP/eval-stdin.php file through its use of the php://input wrapper. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted post request to the target server. Successfully exploiting this vulnerability could result in arbitrary PHP code execution on the target system.

Name	References	Description
Strike Cisco ASA SSL VPN XML Packet Memory Corruption	CWE: 415 CVE: 2018-0101 BID: 102845 EXPLOITDB : 43986	This strike exploits a double-free memory corruption vulnerability in Cisco ASA. The vulnerability is due to failure to parse invalid XML data. By sending a crafted SSL packet containing invalid XML, a remote, unauthenticated attacker could execute arbitrary code on the targeted device.
Strike Cisco Adaptive Security Appliance - Path Traversal	CWE: 20 CVE: 2018-0296 EXPLOITDB : 44956 BID: 104612	This strike exploits a vulnerability of the Cisco Adaptive Security Appliance (ASA) web interface. The vulnerability is due to improper input validation of the HTTP URL. An attacker could exploit this vulnerability by sending a specially-crafted HTTP request to the target device. A successful exploit could allow the attacker to cause a DoS condition or unauthenticated disclosure of information.
Strike H2O Webserver HTTP Headers Buffer Overflow	CWE: 119 CVE: 2018-0608	This strike exploits a heap buffer overflow vulnerability in H2O Webserver. H2O Webserver has a function to allocate sufficient memory for large HTTP headers, however, in certain cases the buffer position pointer may become negative or overly large. In this case, the buffer will not be reallocated, leading to a buffer overflow. An attacker can exploit this vulnerability by sending a specially crafted HTTP message. Successful exploitation may result in arbitrary code execution or abnormal termination of the H2O Webserver, leading to a denial of service condition.
Strike Microsoft Edge Chakra Incorrect Bounds Check	CWE: 119 CVE: 2018-0769 GOOGLE: 1390 EXPLOITDB : 43710 BID: 102396	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that will allow for an integer overflow to occur because a bounds check is calculated incorrectly when the code is JITed. This may lead to a denial of service condition in the browser, or potentially remote code execution.

Name	References	Description
Strike Microsoft Edge Chakra Deferred Parsing Wrong Scope	CWE: 119 CVE: 2018-0775 GOOGLE: 1412 EXPLOITDB : 43717 BID: 102400	This strike exploits a vulnerability in the Microsoft Edge Browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that the DeferParse flag causes an incorrect opcode to be generated, which changes the function expression's scope. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Chakra ASM EmitCall Type Confusion	CWE: 200 CVE: 2018-0780 BID: 102389 GOOGLE: 1433 EXPLOITDB : 43720	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the javascript Chakra engine. The ASM EmitCall function does not properly handle invalid function calls and this can lead to an out of bounds read. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Chakra InitProto Type Confusion	CWE: 119 CVE: 2018-0834 GOOGLE: 1455 EXPLOITDB : 44078 BID: 102859	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in Javascript Chakra engine. It is possible to craft Javascript in such a way that when optimizing InitProto instructions type confusion will occur. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Chakra NewScObjectNoCtor Array Type Confusion	CWE: 119 CVE: 2018-0838 GOOGLE: 1463 EXPLOITDB : 44080 BID: 102877	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that when NewScObjectNoCtor is used to set a new object's __proto__ type confusion can occur. This may lead to a denial of service condition in the browser, or potentially remote code execution.

Name	References	Description
Strike Microsoft Internet Explorer String.lastIndexOf Use After Free	GOOGLE: 1453 CWE: 119 CVE: 2018-0866 BID: 103032 EXPLOITDB : 44153	This strike exploits a vulnerability in the Microsoft Internet Explorer browser. Specifically the vulnerability exists within the Javascript engine. An attacker can craft Javascript in such a way that when invoking the lastIndexOf method on String a Use After Free can occur potentially resulting in memory disclosure. This can lead to a denial of service condition in the browser or potentially remote code execution.
Strike Microsoft Edge Chakra Stack to Heap Copy Fix Bypass	CWE: 119 CVE: 2018-0933 GOOGLE: 1502 EXPLOITDB : 44396 BID: 103274	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that bypasses the fix for a stack to heap copy by adding a line that allocates "head" to the heap. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Internet Explorer jscript.dll Use-After-Free	CWE: 119 CVE: 2018-0935 BID: 103298 EXPLOITDB : 44404	This strike exploits a vulnerability in the Microsoft Internet Explorer browser. The vulnerability lies within jscript.dll. A HTML page containing Javascript can be crafted in such a way that allows for a heap buffer overflow. Successful exploitation may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Edge Chakra Magic Value Type Confusion	CWE: 119 CVE: 2018-0953 GOOGLE: 1531 EXPLOITDB : 44694 BID: 103990	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that the JITed code does not check the input value, which can lead to type confusion. This may lead to a denial of service condition in the browser, or potentially remote code execution.

Name	References	Description
Strike Microsoft Edge Chakra Bounds Check Bypass	CWE: 119 CVE: 2018-0980 GOOGLE: 1530 EXPLOITDB : 44653 BID: 103626	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that it is possible to incorrectly remove a bounds check. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Electron Protocol Handler Command Injection	CWE: 78 CVE: 2018-10000 06 BID: 102796 EXPLOITDB : 43899	This strike exploits a remote command injection vulnerability in GitHub Electron versions 1.8.2-beta.3 and earlier, 1.7.10 and earlier, 1.6.15 and earlier. The vulnerability is due to insufficient validation of whether additional command line arguments were specified via the URI. This vulnerability could allow an unauthorized user to execute arbitrary code on the server.
Strike OpenEMR edit_globals Remote Command Execution	CWE: 78 CVE: 2018-10000 19 EXPLOITDB : 45161	This strike exploits a command injection vulnerability in OpenEMR. The vulnerability is due to improper validation of input passed to 'edit_globals.php' script. By exploiting this vulnerability, a remote authenticated attacker can execute arbitrary OS commands on the target router.
Strike Squid Proxy Server ESI Null Pointer Dereference	CWE: 476 CVE: 2018-10000 27	This strike exploits a null pointer dereference vulnerability in Squid Proxy Server. Due to an implementation error, a null pointer dereference occurs when Squid attempts to fetch HTML fragments from esi:include elements. This dereference results in a segmentation fault, leading to abnormal termination of the Squid process.
Strike Modx Revolution phpthumb Remote Code Execution	CWE: 732 CVE: 2018-10002 07	This strike exploits a remote code execution vulnerability found in Modx Revolution CMS. The vulnerability is due to improper input validation while processing parameters before passing them into 'phpthumb' class. An attacker could exploit this vulnerability by crafting a special HTML POST request that can create a file with custom a filename and content. This can result in execution of arbitrary commands under the privileges of web server daemon user.

Name	References	Description
Strike GitList searchTree method Remote Code Execution	CWE: 20 CVE: 2018-10005 33 EXPLOITDB : 44993	This strike exploits a parameter injection vulnerability found in klaussilveira GitList. The vulnerability is due to insufficient validation of input supplied to php function 'escapeshellarg' within searchTree form. Remote attackers can exploit this vulnerability by crafting a malicious HTTP POST request, ultimately gaining code execution on the target system.
Strike Jenkins Remote Code Execution	CWE: 502 CVE: 2018-10008 61 BID: 106176	This strike exploits a remote code execution vulnerability in Jenkins. The vulnerability is due to improper filtering of the "value" parameter when invoking a method on Java objects. An attacker could exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation results in remote code execution on the target server.
Strike Dolibarr carte.php Reflected XSS	CWE: 79 CVE: 2018-10095	This strike exploits a reflected cross-site scripting vulnerability found in Dolibarr CRM. This vulnerability is due to inadequate input filtering in the web interface, while parsing input passed to foruserlogin parameter within adherents/cartes/carte.php. By exploiting this vulnerability an attacker could cause arbitrary HTML/script code to be executed by the target user's browser.
Strike Trend Micro Endpoint Application Control FileDrop Directory Traversal	CWE: 22 CVE: 2018-10357	This strike exploits a directory traversal vulnerability in the management console of Trend Micro Endpoint Application Control. The vulnerability is due to insufficient validation of filenames in the filename parameter of the Content-Disposition header in multipart/form-data requests sent to FileDropService. A remote, authenticated user can exploit this vulnerability by submitting a crafted request to the target server. Successful exploitation could result in the execution of arbitrary code as the SYSTEM user.
Strike Dasan GPON Home Router GponForm dest_host OS Injection	CWE: 78 CVE: 2018-10562 EXPLOITDB : 44576	An arbitrary file overwrite vulnerability has been identified in Dasan GPON Home Router. The vulnerability is caused by the lack of proper input sanitisation of 'dest_host' parameter within the 'GponForm'. The vulnerability can be exploited by sending a specially-crafted POST request, allowing the attacker to execute arbitrary commands on the device with root privileges.
Strike ProjectPier Remote File Inclusion	CWE: 89 CVE: 2018-10759	This strike exploits a remote file inclusion vulnerability in ProjectPier. The vulnerability is due to improper sanitization of "id" parameter in requests to patch.php script. By exploiting this vulnerability, a remote, unauthenticated attacker could execute arbitrary commands or SQL statements. Note: When run in one-arm mode, this strike will retrieve a malicious sql file from an attacker-controlled web server ( <a href="http://172.16.2.210:8000/mal">http://172.16.2.210:8000/mal</a> ) and execute it on the target.

Name	References	Description
Strike WordPress Plugin Pie Register Blind SQL Injection	CWE: 89 CVE: 2018-10969 EXPLOITDB : 44867	This Strike exploits a blind SQL injection in WordPress Pie Register plugin. The vulnerability is due to insufficient user input sanitization passed to order parameter. A specially crafted HTTP GET request can cause a SQLi in the context of the database user.
Strike Quest KACE System Management Appliance Remote Code Execution	CWE: 78 CVE: 2018-11138	This strike exploits a critical command injection vulnerability within the Quest KACE System Management Appliance. The vulnerability arises from the /common/download_agent_installer.php script's inadequate sanitization of user-supplied input. Specifically, arises due to the the script fails to properly to properly neutralize special elements used in operating system commands, allowing an attacker to inject arbitrary commands. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the vulnerable endpoint, potentially leading to remote code execution.
Strike Moodle CMS questiontype.php Answer Remote Code Execution	CWE: 74 CVE: 2018-1133 EXPLOITDB : 46551 BID: 104307	The strike reproduces a remote code execution attack on Moodle CMS platform. The vulnerability resides in poor user input sanitization for 'answer' parameter within 'questiontype.php', when defining a new quizz of type 'Calculated'. By exploiting the issue, a remote authenticated attacker may execute arbitrary PHP code with HTTP Server privileges.
Strike AXONPBX Web interface Auto-Dialer Agents reflected Cross Site Scripting	CWE: 79 CVE: 2018-11552	This strike exploits a reflected cross-site scripting vulnerability found in AXONPBX Web interface. This vulnerability is due to inadequate input filtering in the web interface, while parsing input passed to name parameter within Auto-Dialer Agents form. By exploiting this vulnerability an attacker could cause arbitrary HTML/script code to be executed by the target user's browser.
Strike Quest Appliance - NetVault Backup Stack Buffer Overflow	CWE: 20 CVE: 2018-1161	A stack buffer overflow has been identified in Quest NetVault Backup appliance. The vulnerability is caused by the lack of proper input sanitisation in the context of multipart HTTP requests processing. The vulnerability can be exploited by accessing the Web Interface of the NetVault server via a specially-crafted HTTP POST request, allowing the attacker arbitrary code execution with SYSTEM privileges.
Strike Quest Appliance - NetVault Backup Arbitrary File Overwrite	CVE: 2018-1162	An arbitrary file overwrite vulnerability has been identified in Quest NetVault Backup appliance. The vulnerability is caused by the lack of user input sanitisation in the context of log exportation. The vulnerability can be exploited by accessing the Web Interface of the NetVault server via a specially-crafted HTTP POST request, allowing the attacker to overwrite any file with SYSTEM privileges.
Strike Quest NetVault Backup Checksession Authentication Bypass	CVE: 2018-1163	This strike exploits an authentication bypass vulnerability in Quest NetVault Backup. The vulnerability is due to insufficient validation of the checksession parameter in multipart HTTP requests. Successful exploitation may result in successful bypass of the authentication mechanism.

Name	References	Description
Strike Ignite Realtime Openfire Reflected Cross Site Scripting	CWE: 79 CVE: 2018-11688	This strike exploits a reflected cross-site scripting vulnerability found in Ignite Realtime Openfire Web interface. This vulnerability is due to inadequate input filtering in the web interface, while parsing input passed to 'url' parameter within login.jsp form. By exploiting this vulnerability an attacker could cause arbitrary HTML/script code to be executed by the target user's browser.
Strike Joomla! CMS Gridbox extension Reflected Cross-Site Scripting	CWE: 79 CVE: 2018-11690	This strike exploits a cross-site scripting vulnerability in Joomla! CMS equipped with Gridbox extension. This vulnerability is due to inadequate input filtering in the web interface, while parsing the input from 'app' and 'category' parameters. By exploiting this vulnerability an attacker could cause arbitrary HTML/script code to be executed by the target user's browser or stole the victim's cookie.
Strike Squid Proxy ESI and OpenSSL Configuration Denial of Service	CWE: 476 CVE: 2018-1172	This strike exploits a code execution vulnerability in Squid Proxy. The vulnerability is due to improper handling of objects in memory within the ESI and OpenSSL functionalities of the server. By sending a crafted ESI responses to the target server, the attacker can cause denial-of-service conditions on the target proxy service.
Strike Apache Tomcat mod_jk JK Status Manager Access Bypass	CWE: 22 CVE: 2018-11759 BID: 105888	This strike exploits an access bypass vulnerability in Apache Tomcat JK Status Manager. By inserting a semicolon after the jkstatus uri, access restrictions are bypassed. An attacker could send specially crafted HTTP GET requests to change ports, resulting in a denial of service condition, or to disclose information about the target server.
Strike Dell EMC VMAX Virtual Appliance Manager Authentication Bypass	CWE: 798 CVE: 2018-1216 BID: 103039	This strike exploits an authentication bypass on Dell EMC VMAX Virtual Appliance Manager. This vulnerability is due to improper use of an account "smc" which is not documented. A remote attacker can exploit this vulnerability by sending hardcoded account and password to the system. Successful exploitation results in authentication bypass on target server.
Strike Mozilla Firefox Javascript Array.Prototype.Push Information Disclosure	CWE: 20 CVE: 2018-12387 BID: 105460	This strike exploits an information disclosure vulnerability in the Mozilla Firefox browser. Specifically, the JavaScript JIT compiler inlines Array.prototype.push with multiple arguments that result in the stack pointer being off by 8 bytes. When this occurs a memory address gets leaked that can be used as part of an exploit. This strike demonstrates the information disclosure by dumping the leaked memory addresses.
Strike iCMS v7.0.8 admincp.php SQL Injection	CWE: 89 CVE: 2018-12498	This strike exploits an Time-Based SQL injection vulnerability in iCMS v7.0.8. The vulnerability is caused by insufficient validation of user input on HTTP requests which are used to create SQL queries. Successful exploitation could allow an attacker to trigger a denial-of-service on the target server for a short period.

Name	References	Description
Strike phpMyAdmin 4.8.1 File Inclusion	CWE: 287 CVE: 2018-12613 EXPLOITDB : 44924 BID: 104532	This strike exploits a file inclusion vulnerability in phpmyadmin 4.8.1. The vulnerability is caused by insufficient validation of user input on HTTP requests which are used to create file include queries. Successful exploitation could allow an attacker to have read/execute access on the target server.
Strike WordPress Plugin iThemes Security SQL Injection	CWE: 89 CVE: 2018-12636 EXPLOITDB : 44943	This Strike exploits a blind SQL injection in WordPress iThemes Security plugin. The vulnerability is due to insufficient user input sanitization passed to 'orderby' parameter. A specially crafted HTTP GET request can cause a SQLi in the context of the database user.
Strike Spring Data Commons Remote Code Execution	CWE: 20 CVE: 2018-1273 BID: 100948	This strike exploits a remote code execution vulnerability in Pivotal Spring Data Commons. The vulnerability is due to a SPEL injection in SimpleEvaluationContext method. Successful exploitation can result in arbitrary code execution in the context of Spring Data Commons.
Strike iCMS v7.0.8 article.admincp.php SQL Injection	CVE: 2018-12888	This strike exploits a Time-Based SQL injection vulnerability in iCMS v7.0.8. The vulnerability is caused by insufficient validation of user input, app=article, on HTTP requests, which are used to create SQL queries. Successful exploitation could allow an attacker to trigger a denial-of-service on the target server for a short period.
Strike WordPress Core Authenticated Directory Traversal	CWE: 22 CVE: 2018-12895 BID: 104569	The strike exploits an authenticated directory traversal vulnerability in WordPress platform. The vulnerability is due to the lack of sanitization of the 'thumb' POST parameter while handling media files metadata within 'post.php', and can be exploited by any account with edit rights. As a consequence, an attacker may delete arbitrary files within the file system which can be leveraged to code execution by changing the platform's configuration.
Strike Zoho ManageEngine Desktop Central Arbitrary File Deletion	CWE: 20 CVE: 2018-12999	This strike exploits an arbitrary file deletion vulnerability in Zoho ManageEngine Desktop Central. The vulnerability is due to insufficient input validation in requests handled by AgentTrayIconServlet. The values of the HTTP parameters are extracted and concatenated to form the file path without any validation for directory traversal characters. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted message to the target server. Successful exploitation could result in the deletion of arbitrary files. This may lead to a denial of service condition if important executables and dynamic link libraries are deleted.

Name	References	Description
Strike Apache Pluto PortletV3Annotated Demo MultipartPortlet Arbitrary File Upload	CWE: 200 CVE: 2018-1306 EXPLOITDB : 45396	A file upload vulnerability was found in Apache Pluto PortletV3AnnotatedDemo. The vulnerability is due to improper access control of user-supplied input when the portlet performs a file-uploading operation. Successful exploitation can result arbitrary file upload and possible remote code execution in the context of the user running the webserver.
Strike TerraMaster NAS URL Reflected XSS	CWE: 79 CVE: 2018-13329	This strike exploits a vulnerability in the TerraMaster NAS device. This device allows for the attacker to inject Javascript in the URL because it does not properly validate pages that do not exist. It is possible for an attacker to perform a Reflected XSS attack by injecting javascript in the requested URL.
Strike TerraMaster NAS groupname Parameter System Command Injection	CWE: 78 CVE: 2018-13330	This strike exploits a vulnerability in the TerraMaster NAS device. This device allows for the option to pass command line arguments to the system during the creation of a user but does not properly validate the arguments passed via the groupname parameter. It is possible to execute system commands as a root user on a vulnerable device.
Strike TerraMaster NAS sysname Parameter HTML Injection	CWE: 79 CVE: 2018-13334	This strike exploits a vulnerability in the TerraMaster NAS device. This device allows for an attacker to execute a cross site scripting attack against the system by performing HTML injection via the sysname parameter. It is then possible to hijack the user session the vulnerable system.
Strike TerraMaster NAS Password System Command Injection	CWE: 78 CVE: 2018-13336	This strike exploits a vulnerability in the TerraMaster NAS device. This device allows for the option to pass command line arguments to the system during the creation of a user but does not properly validate the arguments passed via the password parameter. It is possible to execute system commands as a root user on a vulnerable device.
Strike TerraMaster NAS Username System Command Injection	CWE: 78 CVE: 2018-13338	This strike exploits a vulnerability in the TerraMaster NAS device. This device allows for the option to pass command line arguments to the system during the creation of a user but does not properly validate the arguments passed. It is possible to execute system commands as a root user on a vulnerable device.
Strike TerraMaster NAS checkName System Command Injection	CWE: 78 CVE: 2018-13358	This strike exploits a vulnerability in the TerraMaster NAS device. This device allows for the option to pass command line arguments to the system during the creation of a user but does not properly validate the arguments passed via the checkName parameter. It is possible to execute system commands as a root user on a vulnerable device.
Strike Apache Tika tika-server Remote Command Injection	CVE: 2018-1335 BID: 104001	This strike exploits a post-authentication remote code execution vulnerability found in Apache Tika Server. The vulnerability is due to improper input validation while processing HTTP headers from client requests. An attacker could exploit this vulnerability by crafting a special HTML request, resulting in execution of arbitrary commands under the privileges of the current user.

Name	References	Description
Strike Fortinet FortiOS SSL VPN Credentials Disclosure	CWE: 22 CVE: 2018-13379 EXPLOITDB : 47288 BID: 108693	This strike replicates a directory traversal attack on Fortinet FortiOS. The vulnerability resides in the '/remote/fgt_lang' endpoint and affects product versions 5.6.3 to 5.6.7 and 6.0.0 to 6.0.4. By exploiting this flaw, a remote unauthenticated attacker may take over the device and perform attacks such as DNS hijacks.
Strike Fortinet FortiOS and FortiProxy SSLVPN Web Portal Magic Improper Authorization	CVE: 2018-13382 CWE: 863	This strike exploits an improper authorization vulnerability in SSLVPN web portal of Fortinet FortiOS and FortiProxy. The vulnerability is due to improper authorization of the SSL VPN web portal component in FortiOS and FortiProxy. A remote, unauthenticated attacker could exploit this vulnerability by crafting a HTTP request containing a parameter called "magic" with the value "4tinet2095866". Successful exploitation could allow the attacker to modify the password of SSL VPN web portal in Fortinet FortiOS and FortiProxy.
Strike Xen Project XAPI Update Directory Traversal	CWE: 22 CVE: 2018-14007	This strike exploits a directory traversal vulnerability in the XAPI component of Xen. The vulnerability is due to insufficient handling of URL-encoded path components in requests sent to the pool update endpoint, used for supplying updates to other members of a resource pool. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation results in the disclosure of arbitrary file contents from the server, which may include the administrator token.
Strike SoftNAS Cloud OS Command Injection	CWE: 78 CVE: 2018-14417 BID: 104914	This strike exploits a remote code execution in SoftNAS Cloud. The vulnerability is caused by insufficient validation of 'recentVersion' parameter on HTTP requests. Successful exploitation could allow an attacker to trigger a remote command execution on the target server.
Strike Open-AudIT Community Store Cross Site Scripting	CWE: 79 CVE: 2018-14493 EXPLOITDB : 45160	This strike exploits a store cross-site scripting vulnerability in Open-AudIT Community 2.2.6. This vulnerability is due to improper http input filtering the parameter "groups". By exploiting this vulnerability an attacker could cause arbitrary HTML/script code to be executed by the target user's browser.
Strike ASUSWRT appGet.cgi OS Command Injection	CVE: 2018-14714	A command injection vulnerability exists in ASUSWRT firmware version 3.0.0.4.382.50624 and earlier. The flaw results from lack of user input validation for HTTP parameters on the 'appGet.cgi' path. By sending a crafted 'hook' parameter, a remote attacker may execute arbitrary OS commands as the 'root' user.

Name	References	Description
Strike Cgit web server path Parameter Directory Traversal	CWE: 22 CVE: 2018-14912 EXPLOITDB : 45148	This strike exploits a directory traversal vulnerability in cgit web server. The vulnerability is caused by insufficient validation of user input, path, on HTTP requests. Successful exploitation could allow an attacker to have arbitrary file accessible on target system.
Strike NUUO NVRmini Devices uploaddir OS Command Injection Vulnerability	CVE: 2018-14933 CWE: 78	This strike exploits an OS command injection vulnerability in NUUO NVRmini Devices. The vulnerability is due to improper input validation of parameters used in upgrade_handle.php on NUUO NVRmini devices. A remote, unauthenticated attacker could exploit this vulnerability by crafting a http request containing shell metacharacters in the uploaddir parameter for a writeuploaddir command. Successful exploitation could allow the attacker to perform remote code execution.
Strike OpenEMR manage_site_files Unrestricted File Upload	CWE: 434 CVE: 2018-15139	A file upload vulnerability was found in the OpenEMR. The vulnerability is caused by the lack of proper input sanitisation passed to the manage_site_files Web PHP form. Successful exploitation can result in arbitrary code execution in the context of the user running OpenEMR.
Strike Advantech WebAccess SCADA bwMainLeft.asp Cross-Site Scripting	CWE: 79 CVE: 2018-15707	An unauthenticated stored cross-site scripting vulnerability exists in Advantech WebAccess. The vulnerability resides within 'bwMainLeft.asp' and can be exploited by crafting a GET request containing a malicious 'pname' parameter. By exploiting this vulnerability an attacker could execute arbitrary scripts on the target browser.
Strike Nagios XI Snoopy magpie Remote Code Execution	CVE: 2018-15708	This strike exploits a remote code execution vulnerability in Nagios XI Snoopy component. The vulnerability resides in the lack of request sanitization when parsing the 'url' parameter within 'magpie_debug.php' file. By providing the '-o' flag within the parameter's value, an attacker is able to download a Php script from an arbitrary url and dump it to a publicly accessible path in order to execute commands on the target system.
Strike Nagios XI Unauthenticated Stored Cross-site Scripting	CWE: 79 CVE: 2018-15712	An unauthenticated stored cross-site scripting vulnerability exists in Nagios XI web interface. The vulnerability resides within 'api_tool.php' and can be exploited by crafting a GET request containing a malicious 'host' parameter. The parameter's value is then stored in bpi.conf and is later included in the web management interface. By exploiting this vulnerability an attacker could execute arbitrary scripts on the target browser.
Strike Adobe ColdFusion CKEditor upload.cfm Directory Traversal	CWE: 20 CVE: 2018-15960 BID: 105317	This strike exploits a directory traversal vulnerability in Adobe ColdFusion CKEditor. The vulnerability is due to improper sanitization in the file upload.cfm. An attacker could exploit this vulnerability by sending a crafted HTTP request to the target server. By successfully exploiting this vulnerability, a remote, unauthenticated attacker could upload arbitrary files to the target server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Adobe ColdFusion CKEditor upload.cfm Unrestricted File Upload	CWE: 434  CVE: 2018-15961	This strike exploits an unrestricted file upload vulnerability in Adobe ColdFusion CKEditor. The vulnerability is due to improper restrictions on the files uploaded by users. By successfully exploiting this vulnerability, a remote, unauthenticated attacker could upload arbitrary files and execute them on the target server.
Strike WordPress Plugin Wechat Broadcast 1.2.0 Local File Inclusion	EXPLOITDB : 45438  CWE: 22  CVE: 2018-16283	This strike exploits a remote file inclusion vulnerability in WordPress Plugin Wechat Broadcast 1.2.0. The vulnerability is due to improper sanitization of the "url" parameter. By successfully exploiting this vulnerability, a remote, unauthenticated attacker could retrieve arbitrary files from the target server.
Strike WordPress Plugin Localize 1.0 Local File Inclusion POST	EXPLOITDB : 45439  CWE: 22  CVE: 2018-16299	This strike exploits a remote file inclusion vulnerability in WordPress Plugin Localize My Post 1.0. The vulnerability is due to improper sanitization of the "file" parameter. By successfully exploiting this vulnerability, a remote, unauthenticated attacker could retrieve arbitrary files from the target server.
Strike ManageEngine Desktop Central Search Cross Site Scripting	CWE: 79  CVE: 2018-16833	This strike exploits a cross site scripting vulnerability in ManageEngine's Desktop Central Platform. The vulnerability can be exploited by through malicious input passed via "q" parameter in the search field. By exploiting this flaw, an attacker obtains client-side Javascript code execution within victim's browser which can lead to information disclosure and credentials theft.
Strike LimeSurvey TCPDF phar Deserialization Remote Code Execution	CWE: 502  CVE: 2018-17057  EXPLOITDB : 46634	This strike exploits a remote code execution in LimeSurvey. The vulnerability resides in a PHP Phar deserialization within the 'TCPDF' component and can be exploited by uploading a malicious JPEG/Phar polyglot and exporting the survey that contains it. Exploiting this flaw requires authentication and results in remote code execution.
Strike MyBB Post Video Stored Cross Site Scripting	CWE: 79  CVE: 2018-17128	This strike exploits a stored cross site scripting vulnerability in MyBB platform. The vulnerability can be exploited by crafting a malicious video attachment when creating a new topic. By exploiting this flaw, an attacker obtains client-side Javascript code execution within victim's browser which can lead to information disclosure and credentials theft.
Strike ManageEngine OpManager Search Blind SQL Injection	CWE: 89  CVE: 2018-17243	This strike exploits a blind SQL injection vulnerability in ManageEngine's OpManager application. The vulnerability is present in the global search input field as a result of insufficient user input sanitization. Therefore, an attacker may be able to read arbitrary database records or even access system files, depending on the database's configuration.

Name	References	Description
Strike Elastic Search Server.js Local File Inclusion	CWE: 829 CVE: 2018-17246 BID: 106285	This strike exploits a remote file inclusion vulnerability in Elasticsearch Kibana. The vulnerability is due to improper sanitization of the "apis" parameter. By successfully exploiting this vulnerability, a remote, unauthenticated attacker could retrieve javascript files from the target server. The other file format can be found in a log file on the target server.
Strike Joomla component Questions SQL Injection	CWE: 89 CVE: 2018-17377 EXPLOITDB : 45468	This strike exploits a SQL injection vulnerability in the Questions component for Joomla!. The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this vulnerability by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure.
Strike IBM Identity Governance and Intelligence SQL Injection	CWE: 89 CVE: 2018-1756 EXPLOITDB : 45392	This strike exploits a SQL injection vulnerability in IBM Security Identity Governance Virtual Appliance. The vulnerability is caused by insufficient validation of user input on HTTP requests which are used to create SQL queries. Successful exploitation could allow an attacker to have access of back-end database.
Strike Kubernetes Dashboard Authentication Bypass Information Disclosure	CVE: 2018-18264 CWE: 306	This strike exploits an information disclosure vulnerability in Kubernetes Dashboard. The vulnerability allows unauthorized access to the kubernetes-dashboard-certs secret object. When an HTTP GET request is sent to /api/v1/secret/kube-system/kubernetes-dashboard-certs, access to the kubernetes-dashboard-certs object is not restricted and the server responds with the TLS certificate and private key.
Strike CentOS Web Panel Authenticated OS Command Injection	CWE: 78 CVE: 2018-18322	This strike exploits a remote command execution in CentOS Web Panel. The vulnerability is due to lack of parameter sanitization when executing service-related operations, with the service name passed as a GET parameter. By exploiting this vulnerability, an authenticated attacker is able to execute system commands as a root user.
Strike Mozilla Firefox Custom Elements Object Write After Free	BID: 106781 CWE: 416 CVE: 2018-18500	This strike simulates the traffic caused by exploiting a vulnerability in the Mozilla Firefox browser. Specifically, the vulnerability exists in the 'Custom Elements' stream handler component of Firefox. When handling an HTML5 stream in concert with custom HTML elements, the stream parser object is freed while still in use, leading to a crash. An attacker can exploit this vulnerability by passing a malicious web page to the targeted browser.
Strike LAquis SCADA PAGINA TITULO HTTP Parameter Command Injection	CWE: 74 CVE: 2018-18992 BID: 106634	This strike exploits a command injection vulnerability in LAquis SCADA. The PAGINA parameter in HTTP requests to acompanhamentotela.lhtml and the TITULO parameter in requests to relatorioindividual.lhtml are not sanitized for command injection characters. An attacker can send a specially crafted HTTP GET or POST request to achieve command execution on the target machine.

Name	References	Description
Strike LAquis SCADA NOME HTTP Parameter Command Injection	CWE: 862 CVE: 2018-18996 BID: 106634	This strike exploits a command injection vulnerability in LAquis SCADA. The NOME parameter in HTTP requests to relatorionome.lhtml is not sanitized for command injection characters. An attacker can send a specially crafted HTTP GET or POST request to achieve command execution on the target machine.
Strike Webmin history Parameter Cross-Site-Scripting	CWE: 79 CVE: 2018-19191	This strike exploits a cross-site scripting vulnerability in Webmin. The vulnerability results from the lack of sanitization when displaying the POST parameter 'history' in '/shell/index.cgi'. A successful exploitation leads to arbitrary code execution in visitors' browsers or credentials theft.
Strike PHP-Proxy Local File Inclusion	CWE: 200 CVE: 2018-19246 EXPLOITDB : 45861	This strike simulates an exploitation of a local file inclusion vulnerability present in PHP Proxy. The vulnerability results from the lack of input sanitization when handling the 'q' parameter. By exploiting this flaw, an attacker could read arbitrary files from the server's file system.
Strike OpenMRS Webservices API XML Deserialization Remote Code Execution	CWE: 502 CVE: 2018-19276 EXPLOITDB : 46327	This strike exploits an insecure deserialization via XML payload in OpenMRS's Webservices API module. By exploiting the vulnerability, an unauthenticated attacker might be able to execute system commands in the context of the user running the webserver process.
Strike PHP imap Remote Command Injection	CWE: 78 CVE: 2018-19518	This strike exploits a remote code execution vulnerability in the PHP imap_open function on Ubuntu or Debian. This vulnerability is due to improper handling of the -oProxyCommand values when a client sends http traffic to the server which has some imap functionality. A remote attacker can exploit this vulnerability by sending crafted http requests to the target server. Successful exploitation results in remote code execution. *Note: Actual exploit depends on server config and other parameters, this exploit demonstrate an server with username, password and hostname parameters. Exploit is under hostname parameter.
Strike phpMyAdmin Local File Inclusion	CWE: 200 CVE: 2018-19968	This strike exploits a remote file inclusion vulnerability in phpMyAdmin. The vulnerability is due to an improper filter, and the ability to execute a SQL sentence. By successfully exploiting this vulnerability, a remote, authenticated attacker could retrieve arbitrary files from the target server.
Strike Jenkins getOrCreate Policy Bypass	CWE: 20 CVE: 2018-19990 01	The strike exploits a policy bypass vulnerability in Jenkins CI Server. This vulnerability is due to insufficient validation of login requests by the "getOrCreate" function. By abusing this flaw, an attacker could trigger the removal of the config.xml file from the Jenkins' root directory which results in granting administrator access to anonymous users.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Jenkins Accept-Language Header Directory Traversal	CWE: 20 CVE: 2018-19990 02	The strike exploits an authenticated directory traversal vulnerability in Jenkins CI Server. The vulnerable code resides within Stapler web framework used by Jenkins, and lacks input validation when processing the "Accept-Language" header. The header will be further used to include a language-specific resource by concatenating the header's content to the resource's path. By exploiting the vulnerability, an attacker could read arbitrary sensitive files from the file system.
Strike Zoho ManageEngine OpManager SQL Injection in getGraphData API	CVE: 2018-20173	This strike exploits a SQL injection vulnerability in Zoho ManageEngine OpManager. The vulnerability resides in the getGraphData API due to insufficient validation of input parameters such as name, index, and policyName. Exploiting this flaw allows a remote, authenticated attacker to execute arbitrary SQL commands on the application's database, potentially compromising its integrity and security.
Strike LibreNMS addhost Remote Code Execution	CWE: 78 CVE: 2018-20434 EXPLOITDB : 47044	A remote code execution vulnerability exists in LibreNMS versions prior to 1.46. The vulnerability is a result of improper sanitization when parsing the 'community' HTTP request parameter within 'addhost.inc.php'. A successful attacker is thus able to send specially crafted HTTP requests that could lead to execution of arbitrary commands on the target server.
Strike Oracle WebLogic Server Remote Diagnosis Assistant rda_tfa_ref_date Command Injection	BID: 102640 CVE: 2018-2615	A command injection vulnerability was found in Oracle WebLogic Remote Diagnosis Assistant web interface. The vulnerability is due to improper user supplied sanitization, when input is supplied to the rda_tfa_ref_date menu command. The vulnerability can be exploited by sending a specially crafted HTTP request to the target server. Successful exploitation can result in arbitrary code execution in the context of the Administrator user.
Strike Oracle WebLogic Remote Diagnosis Assistant rda_tfa_hrs Command Injection	CWE: 78 CVE: 2018-2616	This strike exploits a command injection vulnerability in the web console of the Oracle WebLogic Remote Diagnosis Assistant. The vulnerability is due to improper input validation of HTTP parameter hrs_since menu command in the Java class OsUtils, the command string is not properly sanitized for command injection characters. A remote authenticated attacker can exploit this vulnerability by sending a crafted request to the target application. Successful exploitation could lead to arbitrary command execution on the target server with privileges of the Administrator user.
Strike Oracle Hospitality Simphony Directory Traversal	CVE: 2018-2636 BID: 102560 EXPLOITDB : 43960	This strike exploits a path traversal vulnerability in the ProcessDimeRequest module on the Oracle Hospitality Simphony application. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation results in the disclosure of arbitrary file contents from the target server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle WebLogic Server Fusion Middleware File Upload	CVE: 2018-2894	A file upload vulnerability was found in the Oracle WebLogic Server component of Oracle Fusion Middleware. The vulnerability is caused by the lack of proper input sanitisation of the Weblogic Web Service Test Page. Successful exploitation can result in arbitrary code execution in the context of the user running WebLogic.
Strike Trend Micro Control Manager sCloudService GetPassword SQL Injection	CWE: 89 CVE: 2018-3604	This strike exploits an SQL injection vulnerability in the Trend Micro Control Manager. The vulnerability is due to a lack of authentication for accessing the GetPoliciesOfProductType operation and a failure to sanitize the account parameter in the HTTP request. An external, unauthenticated attacker can leverage this vulnerability by sending a crafted HTTP request to the targeted server. Successfully exploiting this vulnerability may result in the execution of arbitrary SQL code within the context of the Network Service user.
Strike Trend Micro IMSVA Management Portal Authentication Bypass	CWE: 522 CVE: 2018-3609	This strike exploits an authentication bypass in Trend Micro InterScan Mail Security Virtual Appliance. The vulnerability is due to insufficient protection of a log file which is publicly accessible containing session credentials for authenticated users. A remote, unauthenticated attacker can exploit this vulnerability by accessing the diagnostic log and obtaining valid session IDs which can then be used to log in as the associated user without knowledge of the user's credentials, bypassing the standard authentication mechanisms. Successful exploitation results in the bypass of authentication for access to the administrative interface.
Strike TP-Link TL-R600VPN Directory Traversal Information Disclosure	CWE: 22 CVE: 2018-3949	This strike exploits a directory traversal vulnerability in TP-Link TL-R600VPN router. The vulnerability can be exploited by issuing GET requests to the '/help' path. Since the webserver runs with root privileges, an attacker may gain access to the contents of any file residing on the file system.
Strike Apple Safari WebKit WebCore jsElementScrollHeightGetter Use After Free	CWE: 416 CVE: 2018-4200 GOOGLE: 1525 BID: 103961 EXPLOITDB : 44566	This strike exploits a vulnerability in Apple Webkit JavaScriptCore. Specifically, a Use After Free occurs when the jsElementScrollHeightGetter function is invoked in a specific manner. When this happens a denial of service condition, or potentially remote code execution, may occur.

Name	References	Description
Strike Apple Webkit handleMenuItemSelected Use After Free	CWE: 416 CVE: 2018-4312 GOOGLE: 1603 EXPLOITDB : 45481	This strike exploits a vulnerability in Apple Safari Webkit. It is possible to craft javascript and html in such a way that when calling the handleMenuItemSelected method a use after free vulnerability will occur. This can lead to a denial of service condition in the browser, or potentially allow for remote code execution.
Strike Apple Safari Webkit updateReferencedText Use After Free	CWE: 416 CVE: 2018-4315 GOOGLE: 1604	This strike exploits a vulnerability in Apple Safari Webkit. Specifically, it is possible to craft Javascript in such a way that allows for a use-after-free vulnerability to occur when calling the updateReferencedText method. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Apple Safari WebKit handleIntrinsicCall Type Confusion	CWE: 119 CVE: 2018-4382 GOOGLE: 1656	This strike exploits a vulnerability in Apple Safari Webkit. Specifically the vulnerability exists in the ByteCodeParser::handleIntrinsicCall method. It is possible to craft Javascript in such a way that will cause type confusion to occur. This can lead to a denial of service or potentially allow for remote code execution to occur.
Strike Apple Safari WebKit hoistSloppyModeFunctionIfNecessary Improper Object Validation	CWE: 119 CVE: 2018-4386 GOOGLE: 1665	This strike exploits a vulnerability in Apple Safari Webkit. Specifically the vulnerability exists in the BytecodeGenerator::hoistSloppyModeFunctionIfNecessary method. It is possible to craft Javascript in such a way that allows for an object to be passed as the property variable directly as a string to the op_get_direct_pname handler without being properly validated. This can lead to a denial of service in the browser application or potentially allow for remote code execution to occur.
Strike Apple Safari WebKit JSPropertyNameEnumerator Type Confusion	CVE: 2018-4416 CWE: 119 GOOGLE: 1652	This strike exploits a vulnerability in Apple Webkit. Specifically, an attacker can craft JavaScript in such a way that when a for loop is executed and a JSPropertyNameEnumerator object is created, the structure IDs inside the JSPropertyNameEnumerator object can get reused after their parents have been freed leading to type confusion. This can potentially lead to a denial of service or allow for remote code execution in the context of the current running process.
Strike Apple Safari Webkit JIT Allows for Array Proxy Object in Prototype Chains	CWE: 119 CVE: 2018-4438	This strike exploits a vulnerability in Webkit. Specifically, it is possible to create an array having a Proxy object in the prototype chain. This may cause a denial of service condition in the browser or allow for remote code execution to occur.

Name	References	Description
Strike Apple Webkit shiftCountWithArray Storage Out of Bounds Read-Write	CWE: 119 CVE: 2018-4441 GOOGLE: 1685	This strike exploits a vulnerability in Apple Webkit. It is possible to craft Javascript in such a way that an Out of Bounds Read/Write can occur in shiftCountWithArrayStorage. This can cause memory corruption to occur leading to a denial of service in the browser or potentially lead to remote code execution.
Strike WebKit JSC AbstractValue Set Use After Free	CWE: 119 CVE: 2018-4443 EXPLOITDB : 46071	This strike exploits a vulnerability in Apple WebKit. Specifically, the vulnerability exists in the AbstractValue Set method. Javascript can be crafted in such a way that the attacker can write into the immutable butterfly of a Copy on Write array. This can lead to a use after free condition causing a denial of service or potentially lead to remote code execution.
Strike Mozilla Firefox WebAssembly Table Object Integer Underflow	BID: 102786 CWE: 119 CVE: 2018-5093	This strike exploits a vulnerability in the Mozilla Firefox browser. Specifically, the vulnerability exists in the WebAssembly component of Firefox. When handling a table object, the get and set methods are not properly validated. It is possible for a user to provide a value to the index argument of one of these methods to access random memory in the heap buffer of where this table object is stored. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Advantech WebAccess Node chkLogin SQL Injection	BID: 102781 CWE: 89 CVE: 2018-5443	This strike exploits a SQL injection vulnerability in Advantech WebAccess Node. The vulnerability is due to lack of proper validation of user-supplied data used to construct SQL queries. A specially crafted HTTP request could allow the attacker to access and modify sensitive information within the SQL database.
Strike Advantech WebAccess SCADA certUpdate.asp Directory Traversal	BID: 102781 CWE: 22 CVE: 2018-5445	An arbitrary file overwrite vulnerability has been identified in Advantech WebAccess SCADA web platform. The vulnerability is caused by the lack of proper input sanitisation of the certUpdate.asp filename parameter. The vulnerability can be exploited by sending a specially-crafted request, allowing the attacker to execute code on the remote machine with the privileges of the application process.
Strike Epson AirPrint Cross-Site Scripting (XSS)	CWE: 79 CVE: 2018-5550	This strike exploits a cross-site scripting vulnerability in Epson's web configuration page for AirPrint in certain Epson printer products. This vulnerability is due to inadequate input filtering in INPUTT_GEOLOCATION parameter. By exploiting this vulnerability an attacker could execute arbitrary scripts on the target machine.

Name	References	Description
Strike GitStack BasicAuth Header Unauthenticated Remote Code Execution	CWE: 20 CVE: 2018-5955 EXPLOITDB : 44356	This strike exploits a remote code execution vulnerability in GitStack. The vulnerability is due to lack of authentication check when users send a HTTP create user request and improper validation of user-supplied input. By exploiting this vulnerability, a remote, unauthenticated attacker can execute arbitrary PHP code on the target server. NOTE: When run in one-arm mode, this strike creates a backdoor script at /web/backdoor.php.
Strike Joomla SimpleCalendar Catid Array SQL Injection	CWE: 89 CVE: 2018-5974 EXPLOITDB : 44126	This strike exploits an SQL injection vulnerability in the SimpleCalendar component for Joomla!. The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure.
Strike Joomla Aist SQL Injection	CWE: 89 CVE: 2018-5993 EXPLOITDB : 44106	This strike exploits an SQL injection vulnerability in the Aist component for Joomla! The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure.
Strike Joomla Project Log Search SQL Injection	CWE: 89 CVE: 2018-6024 EXPLOITDB : 44124	This strike exploits an SQL injection vulnerability in the Project Log 1.5.3 for Joomla! The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure.
Strike Google Chrome V8 Object Allocation Size Integer Overflow	CWE: 190 CVE: 2018-6065 GOOGLE: 1526 EXPLOITDB : 44584 BID: 103297	This strike exploits a vulnerability in the Google Chrome browser. Specifically, the vulnerability exists in the Google Chrome V8 javascript engine. By passing a prototype chain of objects with a large expected_no_of_properties the instance_size value can be controlled. An integer overflow results in too small of a value being used causing memory corruption to occur. This may lead to a denial of service condition in the browser, or potentially remote code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Google Chrome V8 AwaitedPromise Update Bug	GOOGLE: 1521 CWE: 19 CVE: 2018-6106 BID: 103917	This strike exploits a vulnerability in the Google Chrome browser. Specifically the vulnerability exists within the Javascript V8 engine. An attacker can craft Javascript in such a way that the AwaitedPromise method can be replaced with user Javascript through the use of a then getter. This may lead to an incorrect state in the generator, which can lead to a denial of service condition in the browser or potentially remote code execution.
Strike Trend Micro Email Encryption Gateway searchEmail SQL Injection	CWE: 89 CVE: 2018-6230 EXPLOITDB : 44166	This strike exploits an SQL injection vulnerability in Trend Micro Email Encryption Gateway. The vulnerability is due to the improper sanitization of searching string sent to searchEmail.jsp script. An attacker could exploit this by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure, database corruption, denial of service and others.
Strike Easy Hosting Control Panel op Parameter Reflected Cross-Site Scripting	CWE: 79 CVE: 2018-6361	This strike exploits a cross-site scripting vulnerability in Easy Hosting Control Panel. This vulnerability is due to improper sanitization of "op" parameter controlled by users in HTTP requests. By enticing an authenticated user to visit an attacker controlled webpage or click a malicious link, an attacker could manipulate database, add backdoor accounts, access any cookies, session tokens, or other sensitive information retained by the browser.
Strike Easy Hosting Control Panel domainop Action Parameter Reflected Cross-Site Scripting	CWE: 79 CVE: 2018-6362	This strike exploits a cross-site scripting vulnerability in Easy Hosting Control Panel. This vulnerability is due to improper sanitization of "domainop" action parameter controlled by users in HTTP requests. By enticing an authenticated user to visit an attacker controlled webpage or click a malicious link, an attacker could access any cookies, session tokens, or other sensitive information retained by the browser.
Strike Joomla! Hathor Postinstall Message SQL Injection	CWE: 89 CVE: 2018-6376 BID: 102916	This strike exploits an SQL injection vulnerability in Joomla! CMS. The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure, database corruption, denial of service and others.
Strike Joomla! com_fields Cross-Site Scripting (XSS)	CWE: 79 CVE: 2018-6377 BID: 102917	This strike exploits a cross-site scripting vulnerability in Joomla! CMS. This vulnerability is due to inadequate input filtering in com_fields. By exploiting this vulnerability an attacker could execute arbitrary scripts on the target machine.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike D-Link Router Soapcgi Remote Code Execution	CWE: 78 CVE: 2018-6530	This strike exploits an OS command injection vulnerability in the web component of D-Link. The vulnerability is due to a flaw in the SOAP controlType URL interface. A remote unauthenticated attacker could exploit this vulnerability by sending a specially formatted SOAP request to the target system. Successful exploitation of this vulnerability could result in arbitrary command execution on the target system with root privileges.
Strike AMD Raptr execute_installer Remote File Execution	CWE: 287 CVE: 2018-6546 EXPLOITDB : 44476	This strike exploits a remote file execution vulnerability in AMD Raptr. HTTP POST requests to the execute_installer URI are intended to execute the installer file with path stored in the data parameter. However, any arbitrary executable path stored in the data parameter will be executed. An attacker can send a specially crafted HTTP POST request to cause arbitrary file execution on the target system.
Strike Joomla DT Register SQL Injection	CWE: 89 CVE: 2018-6584 EXPLOITDB : 44108	This strike exploits an SQL injection vulnerability in the DT Register 3.2.7 component for Joomla! The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure.
Strike Belkin Wemo Insight Smart Plug Stack Buffer Overflow	CWE: 787 CVE: 2018-6692	This strike exploits a buffer overflow vulnerability in the Belkin Wemo Smart Plug. Specifically a stack buffer overflow occurs inside the WemoApp libUPnPHandler.so library. When an attacker sends a UPnP packet with a specially crafted EnergyPerUnitCostVersion field a crash may occur. It is possible to execute code remotely on the compromised device as the root user, and because the device uses UPnP it is also possible to use the device to attack and control other smart devices like TVs.
Strike Joomla Saxum Picker SQL Injection	CWE: 89 CVE: 2018-7178 EXPLOITDB : 44136	This strike exploits an SQL injection vulnerability in the Saxum Picker 3.2.10 component for Joomla! The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure.
Strike Joomla Component Saxum Astro SQL Injection	CWE: 89 CVE: 2018-7180 EXPLOITDB : 44133	This strike exploits an SQL injection vulnerability in the Saxum Astro 4.0.14 component for Joomla! The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Google Golang GET Command Injection	CWE: 78  CVE: 2018-7187	This strike exploits a command execution vulnerability in Google Golang client. The vulnerability is due to insufficient sanitization of user input by the go get command. An authenticated attacker can entice the client to use "go get" on a malicious URL, a successful exploitation could result in a command injection on the target user.
Strike Homematic CCU2 2.29.23 - Remote Command Execution	CVE: 2018-7297  EXPLOITDB : 44368	This strike exploits a code execution vulnerability in the HomeMatic CCU2 control unit. This vulnerability is due to improper sanitization for the HTTP header when server sends http traffic back to client. A remote attacker can trigger this vulnerability by sending malicious request to web interface, results in read/write access and execute system commands on the target device.
Strike Joomla component Alexandria Book Library SQL Injection	CWE: 89  CVE: 2018-7312  EXPLOITDB : 44162	This strike exploits a SQL injection vulnerability in the Alexandria Book Library component for Joomla!. The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this vulnerability by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure.
Strike Joomla CW Tags Searchtext SQL Injection	CWE: 89  CVE: 2018-7313  EXPLOITDB : 44158	This strike exploits an SQL injection vulnerability in the CW Tags for Joomla! The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure.
Strike Joomla Component Proclaim Backup File Download	CWE: 200  CVE: 2018-7317  EXPLOITDB : 44159	This strike exploits a file download vulnerability in Joomla! Component Proclaim. The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could download sql files under backup folder via direct requests.
Strike Joomla component CheckList SQL Injection	CWE: 89  CVE: 2018-7318  EXPLOITDB : 44163	This strike exploits an SQL injection vulnerability in the CheckList component for Joomla!. The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure.

Name	References	Description
Strike Site Editor WordPress Plugin - Local File Inclusion	CWE: 200 CVE: 2018-7422 EXPLOITDB : 44340	This strike exploits a local file inclusion vulnerability in Site Editor WordPress plugin. The vulnerability is due to improper sanitization of "ajax_path" parameter in requests to ajax_shortcode_pattern.php script. By exploiting this vulnerability, a remote, unauthenticated attacker could retrieve arbitrary files from the target server. Note: When run in one-arm mode, this strike will retrieve the content of /etc/passwd file. The vulnerable ajax_shortcode_pattern.php script must be available at default location ( <a href="http://[server]/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php">http://[server]/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php</a> ).
Strike TestLink Unauthenticated Remote Code Execution	CWE: 94 CVE: 2018-7466 EXPLOITDB : 44226	This strike exploits a code injection vulnerability in TestLink Open Source Test Management. The vulnerability is due to improper sanitization and handling of user-controlled values passed for "TestLink DB login" parameter in "installNewDB.php" script. By exploiting this vulnerability, a remote, unauthenticated attacker can inject and execute arbitrary PHP code on the target server. NOTE: When run in one-arm mode, a Mysql server must be accessible at "localhost" and user "root" with password "12345" must be configured. Also a database called "testlink" must be created and Mysql must be configured to accept usernames longer than 16 characters.
Strike FasterXML jackson-databind Insecure Deserialization	CWE: 184 CVE: 2018-7489 BID: 103203	This strike exploits an insecure deserialization vulnerability in FasterXML jackson-databind. The vulnerability is due to improper validation of user input used in deserialization and instantiation of Java objects. This is an incomplete fix for CVE-2017-7525. By sending a maliciously crafted JSON input, an attacker could achieve remote code execution in the context of the vulnerable application.
Strike Cgit web server Directory Traversal	CWE: 22 CVE: 2018-7490 EXPLOITDB : 44223	This strike exploits a directory traversal vulnerability in uWSGI PHP plugin. The vulnerability is caused by insufficient validation of user input on HTTP requests. Successful exploitation could allow an attacker to have arbitrary file accessible on target system.
Strike Advantech WebAccess NMS Download Action Directory Traversal	CWE: 22 CVE: 2018-7503 BID: 104190	An arbitrary file overwrite vulnerability has been identified in Advantech WebAccess NMS. The vulnerability is caused by the lack of proper input sanitisation on file paths within DownloadAction servlet. The vulnerability can be exploited by sending a specially-crafted request, allowing the attacker to read arbitrary files.
Strike Drupal Core PHP Deserialization Remote Code Execution	BID: 103534 CWE: 20 CVE: 2018-7600	This strike exploits a vulnerability in Drupal Core open-source CMS. The vulnerability is due to improper validation of user-supplied data while performing server-side deserialization of PHP objects. A malicious user can exploit this vulnerability by sending multiple HTTP POST requests including serialized PHP objects. When successfully exploited, the vulnerability results in complete compromise of the target server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Drupal Core Form Rendering Remote Code Execution	CVE: 2018-7602 BID: 103985	This strike exploits a remote code execution flaw in Drupal Core. This vulnerability is due to improper handling of the HTTP parameter when a client sends http traffic to the server. A remote attacker can exploit this vulnerability by sending crafted http requests to the target server. Successful exploitation results in remote code execution.
Strike Sitecore CMS LogViewerDetails Directory Traversal	CWE: 22 CVE: 2018-7669	This strike exploits a path traversal vulnerability in Sitecore CMS. The vulnerability is due to insufficient validation of 'file' parameter processed in LogViewer application. Remote attackers can exploit this vulnerability by crafting a malicious HTTP request, ultimately gaining access to read arbitrary files.
Strike Schneider Electric U.motion Builder Directory Traversal	CWE: 20 CVE: 2018-7787 BID: 104447	This strike exploits a directory traversal vulnerability in Schneider Electric U.motion Builde. The vulnerability is due to improper validation of input of context parameter in HTTP GET request, which could allow the disclosure of sensitive information.
Strike Schneider Electric IIoT Monitor Zip Directory Traversal	CWE: 434 CVE: 2018-7836	This strike exploits a directory traversal vulnerability in Schneider Electric IIoT Monitor. The vulnerability is due to insufficient handling of directory traversal characters in uploaded ZIP archives uploaded to several endpoints - ProtectionMgmt, RecoveryMgmt, and UpgradeMgmt. An authenticated attacker can exploit this weakness by uploading a crafted ZIP file, allowing them to traverse directories and write arbitrary files to locations accessible by SYSTEM. This vulnerability poses a significant risk of arbitrary code execution.
Strike Schneider Electric U.Motion Builder 1.3.4 Command Injection	CWE: 89 CVE: 2018-7841	An OS command injection exists in Schneider Electric U.Motion Builder. The flaw, located in 'track_import_export.php', is a result of lack of user-supplied data sanitization and may be exploited via the 'object_id' parameter. A remote unauthenticated attack may lead to arbitrary OS commands being issued on the host system.
Strike Zoho ManageEngine Applications Manager 13.5 - Command Injection	CWE: 78 CVE: 2018-7890 BID: 103358	This strike exploits a remote code execution on Zoho ManageEngine Applications Manager 13.5. This vulnerability is due to improper handling of the UserName values under HTTP parameter when a client sends http traffic to the server. A remote attacker can exploit this vulnerability by sending crafted http requests to the target server. Successful exploitation results in remote code execution.
Strike Apache ActiveMQ Reflected Cross Site Scripting	CWE: 79 CVE: 2018-8006	A reflected cross side scripting vulnerability is present in Apache ActiveMQ. The vulnerability takes advantage of "QueueFilter" parameter that is transmitted when performing searches for queues. By exploiting this flaw, an attacker obtains client-side Javascript code execution within victim's browser which can lead to information disclosure and credentials theft.

Name	References	Description
Strike Apache CouchDB_config Command Execution	CWE: 20 CVE: 2018-8007 BID: 104741	This strike exploits a remote code execution in Apache CouchDB. The vulnerability is caused by insufficient validation of administrator supplied configuration settings on HTTP requests. Successful exploitation could allow an attacker to trigger a remote command execution on the target server.
Strike Apache Superset Import Dashboards Remote Code Execution	CWE: 502 CVE: 2018-8021 EXPLOITDB : 45933	A remote code execution exists in Apache Superset through the 'Import Dashboards' feature. The vulnerability exists as a result of an insecure 'pickle' deserialization, allowing execution of arbitrary methods from the Python library. An authenticated attacker can therefore execute arbitrary code on the target system under the user that runs the 'gunicorn' webserver.
Strike Cobub Razor channel_name POST SQL Injection	CWE: 89 CVE: 2018-8057 EXPLOITDB : 44454	An SQL injection vulnerability exists in Cobub Razor mobile analytics appliance. The vulnerability is due to insufficient user-supplied input validation within channel.php script. The successful exploitation of this vulnerability can result in database information disclosure without authentication via a specially crafted HTTP POST request.
Strike Datalust Seq - Authentication Bypass	CWE: 287 CVE: 2018-8096 EXPLOITDB : 45136	This strike exploits an authentication bypass on Datalust Seq web server. This vulnerability is due to improper use of a HTTP parameter "Name:isauthenticationenabled" under HTTP PUT request. A remote attacker can exploit this vulnerability by sending crafted HTTP PUT request to the system. Successful exploitation results in authentication bypass on target server.
Strike Microsoft Edge Chakra BoundFunction NewInstance Out of Bounds Read	CWE: 119 CVE: 2018-8139 EXPLOITDB : 45012 BID: 103977 GOOGLE: 1569	This strike exploits a vulnerability in the Microsoft Edge Browser. Specifically, the vulnerability exists when the BoundFunction::NewInstance function is used to handle calls to a bound function. This method allocates a new argument array and copies the arguments into the new argument array. It will call the function without respecting the CallFlags_ExtraArg flag that indicates that there's an extra argument at the end of the array. This then results in the new array size being one less than what is required, leading to an Out of Bounds memory read. This can cause a denial of service condition in the browser or potentially lead to remote code execution.

Name	References	Description
Strike Microsoft Edge Chakra Heap Buffer Overflow	CWE: 200 CVE: 2018-8145 EXPLOITDB : 45011 BID: 103986	This strike exploits a vulnerability in the Microsoft Edge browser. It is possible to cause a heap buffer to overflow by creating new objects with specific elements as arguments that repeat in javascript. When this code is executed a buffer overflows and a denial of service condition occurs. Remote code execution may also be possible.
Strike Windows VBScript Engine Use After Free	CWE: 119 CVE: 2018-8174	This strike exploits a vulnerability in Microsoft VBScript Engine. Specifically the vulnerability fakes and overrides the array object to perform arbitrary address reading and writing. In the end, it releases code to execute after constructing an object. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.
Strike Microsoft Edge Browser Chakra Parameter Scope Parsing Type Confusion	CWE: 119 CVE: 2018-8279 GOOGLE: 1570 BID: 104641 EXPLOITDB : 45214	This strike exploits a vulnerability in the Microsoft Edge Browser. Specifically the vulnerability exists inside the Microsoft Chakra Javascript engine. It is possible to craft invalid Javascript that still gets parsed by the Chakra engine, which can result in type confusion in the InterpreterStackFrame::OP_ResumeYield method. This can cause a denial of service in the browser or potentially lead to remote code execution.
Strike Microsoft Edge ImplicitCallFlags Intl Check Bypass	CWE: 119 CVE: 2018-8288 GOOGLE: 1565	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically an attacker can craft javascript in such a way that allows for the initialization process to run without caring about the ImplicitCallFlags. This can cause a denial of service condition in the browser or potentially allow for remote code execution to occur.
Strike Microsoft Edge DictionaryPropertyDescriptor CopyFrom Type Confusion	GOOGLE: 1576 CWE: 119 CVE: 2018-8291 BID: 104637 EXPLOITDB : 45215	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically the vulnerability exists within the Javascript Chakra engine. An attacker can craft Javascript in such a way that the CopyFrom method does not copy all fields, including the IsShadowed field, from another descriptor to "this". This causes type confusion to occur, and can lead to a denial of service condition in the browser or potentially remote code execution.

Name	References	Description
Strike Windows VBScript Engine Preserve Array Use After Free	CWE: 119 CVE: 2018-8373	This strike exploits a vulnerability in Microsoft VBScript Engine. Specifically the vulnerability fakes and overrides the array object to perform arbitrary address reading and writing. In the end, it releases code to execute after constructing an object. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.
Strike Microsoft Edge Chakra PathTypeHandlerBase SetAttributesHelper Type Confusion	CWE: 119 CVE: 2018-8384 EXPLOITDB : 45431 BID: 104981 GOOGLE: 1586	This strike exploits a vulnerability in the Microsoft Edge Browser. Specifically, a type confusion vulnerability exists in the Chakra Javascript engine. When object header inlining is deoptimized, the type handler of the object is converted to a dictionary type handler. However, not all attributes belong to the dictionary type, and they are not taken into consideration. If these types are added or removed type confusion will occur. This can lead to a denial of service condition in the browser, or potentially allow for remote code execution.
Strike Microsoft Edge Open With Remote Command Execution	CWE: 20 CVE: 2018-8495 BID: 105461	This strike exploits a remote command execution in Microsoft Edge browser. The vulnerability is due to lack of parameter sanitization when running an external application with a crafted hyperlink as an argument. A user accessing an arbitrary page can be enticed to run a malicious script with a minimum of interaction, allowing the attacker to execute arbitrary commands on the system.
Strike Microsoft VBScript VariantClear Use After Free	CWE: 416 CVE: 2018-8544 GOOGLE: 1659 EXPLOITDB : 45923 BID: 105787	This strike exploits a vulnerability in the Microsoft Internet Explorer Browser. Specifically, the vulnerability exists in VBScript. If a Variant is an object, the object destructor is going to be called and the variant type will be unset. It is possible for the object destructor to then call the attacker controlled code to free the memory holding the variant, and if called upon later a use after free condition will occur. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft VBScript rtFilter Out of Bounds Read	CWE: 119 CVE: 2018-8552 GOOGLE: 1666 EXPLOITDB : 45924 BID: 105786	This strike exploits a vulnerability in the Microsoft Internet Explorer Browser. Specifically, the vulnerability exists in the VBScript component. An input array can be resized during an rtFilter call causing an out of bounds memory read to occur. This may lead to a denial of service condition in the browser, or potentially remote code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Edge Chakra InlineArrayPush InlineArrayPop Type Confusion	CWE: 119 CVE: 2018-8617 BID: 106112 EXPLOITDB : 46202	This strike exploits an vulnerability in the Microsoft Edge browser. Specifically the vulnerability exists inside the Javascript Chakra engine. It is possible to craft Javascript in such a way that when a push or pop method is used on an object with a numeric property the associated InlineArrayPop or InlineArrayPush instruction is called. It is possible to cause type confusion allowing for a denial of service condition to occur or potentially remote code execution.
Strike Microsoft VBScript SafeArray Reference Leak and Use After Free	CWE: 119 CVE: 2018-8625 BID: 106122 GOOGLE: 1668 EXPLOITDB : 46022	This strike exploits a vulnerability in the Microsoft Internet Explorer browser. Specifically, the vulnerability exists in the VBScript engine. It is possible to create VBScript in such a way that can allow for a use-after-free condition to occur when a pointer to a SafeArray object is created and stored and the object is then destroyed. This may lead to a denial of service condition in the browser, or potentially remote code execution.
Strike Microsoft Windows - jscript! JsArrayFunctionHeapSort Out-of-Bounds Write	CWE: 119 CVE: 2018-8631 EXPLOITDB : 46001	This strike exploits a vulnerability in the Microsoft Internet Explorer Out-Of-Bound write. Specifically, the vulnerability exists in the Javascript JsArrayFunctionHeapSort. It is possible to craft Javascript in such a way that will cause a denial of service condition in the browser.
Strike Nagios XI helpedit.php SQL Injection	CWE: 89 CVE: 2018-8734 EXPLOITDB : 44560	This strike exploits an SQL injection vulnerability in Nagios XI. The vulnerability is caused by insufficient validation of user input on HTTP requests which are used to create SQL queries. Successful exploitation could allow an attacker read/write abilities to sensitive information in target server.
Strike Kodi Create Playlist Persistent Cross-Site Scripting (XSS)	CWE: 79 CVE: 2018-8831 EXPLOITDB : 44487	This strike exploits a cross-site scripting vulnerability in Kodi Media Player software. This vulnerability is due to inadequate input filtering in the web interface, while creating a new playlist. By exploiting this vulnerability an attacker could cause arbitrary HTML/script code to be executed by the target user's browser.

Name	References	Description
Strike Easy File Sharing WebServer UserID Remote Buffer Overflow	CWE: 119 CVE: 2018-9059 EXPLOITDB : 44485	This strike exploits a remote buffer overflow vulnerability in Easy File Sharing (EFS) Web Server. The vulnerability is due to insufficient validation of UserID parameter within forum.ghp. Remote attackers can exploit this vulnerability by crafting a malicious login request, ultimately gaining code execution on the target system with elevated privileges.
Strike Zoho ManageEngine OpManager OpManagerFailover Util customerName SQL Injection	CWE: 89 CVE: 2018-9088	This strike exploits an SQL injection vulnerability that exists in ManageEngine OpManager. The vulnerability results from a lack of input validation of the customerName request parameter and a lack of authentication for accessing FailOverHelperServlet servlet. A remote unauthenticated attacker could exploit this vulnerability by sending an HTTP request with a crafted customerName parameter. If the exploitation is successful, the server will execute a maliciously injected SQL statement, which may lead to data tampering in the OpManagerDB backend database and ultimately to the execution of arbitrary code with the privileges of database process.
Strike ManageEngine Recovery Manager Plus Persistent Cross-Site Scripting	BID: 103773 CWE: 79 CVE: 2018-9163 EXPLOITDB : 44666	This strike exploits a cross-site scripting vulnerability in ManageEngine Recovery Manager Plus software. This vulnerability is due to inadequate input filtering in the web interface, while creating a new technician within the technicianAction.do form. By exploiting this vulnerability an attacker could cause arbitrary HTML/script code to be executed by the target user's browser.
Strike Jquery File Upload Arbitrary File Upload	CWE: 434 CVE: 2018-9206 EXPLOITDB : 45584 BID: 105679	This strike exploits an arbitrary file upload vulnerability in BlueImp Jquery File Upload widget. The vulnerability is due to the complete lack of server-side authorization or sanitization when handling a file upload. An attacker is thus able to create arbitrary files on the server which in most cases leads to remote arbitrary code execution.
Strike OpenEMR multiple SQL Injection	CWE: 89 CVE: 2018-9250	This strike exploits a SQL injection in OpenEMR open-source project. The vulnerability is due to insufficient user input sanitization passed through the URI, addressing various PHP scripts. A specially crafted HTTP GET request can cause a SQLi in the context of the database user.
Strike Roundcube Webmail archive.php IMAP Command Injection	CWE: 20 CVE: 2018-9846	This strike exploits a command injection vulnerability in the Roundcube Webmail. This vulnerability is due to improper handling of the HTTP parameter when a client sends http traffic to the server. A remote attacker can trigger this vulnerability by enticing an authenticated user to visit a crafted page, which sends a request to the target server. This results in arbitrary IMAP injection on the target device.

Name	References	Description
Strike SonicWall XML-RPC Remote Code Execution	CWE: 20 CVE: 2018-9866	This strike exploits a remote code execution on SonicWall Global Management System. The vulnerability is due to lack of string sanitization when updating the system's timezone via a crafted XML file. An attacker exploiting the flaw has complete access to the system as the root user.
Strike Apache Solr Config API Insecure Deserialization	CWE: 502 CVE: 2019-0192	This strike exploits an insecure deserialization vulnerability in Apache Solr. The vulnerability is due to insufficient sanitization of requests made to the Config API. This vulnerability can be exploited by sending a specially crafted HTTP request to the Config API. Successful exploitation could lead to remote code execution within the context of the server.
Strike Apache Solr DataImportHandler Code Execution	CWE: 287 CVE: 2019-0193	This strike exploits a script injection vulnerability in Apache Solr via "dataConfig" parameter in the DataImportHandler module. DataImportHandler (DIH) module allows the user to pull in data from databases and other sources. The "dataConfig" parameter allows to specify the entire DIH config as a request parameter. Since a DIH config can contain scripts, this allows the attacker to construct a threatening request on the server. Successful exploitation will result in code execution, in the context of the user running the Apache Solr service.
Strike Apache Struts2 ValueStack OGNL Remote Command Execution	CWE: 915 CVE: 2019-0230	This strike exploits a remote code execution vulnerability found in Apache Struts2 Framework. The vulnerability is due to the lack of input validation leading to a forced double Object Graph Navigation Library (OGNL) evaluation for raw user input. The vulnerability can be exploited by crafting a malicious HTTP POST request. Successful exploitation may result in executing arbitrarily code within the context of the user running the webservice.
Strike Apache Tomcat CGI enableCommandLineArguments Windows Command Injection	CWE: 20 CVE: 2019-0232 BID: 107906	This strike replicates an attack on Apache Tomcat based on a Windows command injection vulnerability. The flaw resides in the way the command arguments for a CGI script are transmitted from the request's parameters on the Windows OS. By exploiting this vulnerability, a remote unauthenticated attacker can execute commands on the host system.
Strike Apache Struts2 ParentFile.Writable File Upload Denial of Service	CVE: 2019-0233 CWE: 835	This strike exploits a file upload vulnerability in Apache Struts2. When an attacker sends an HTTP request with a crafted parameter to the server a denial of service condition on the file upload functionality will occur.

Name	References	Description
Strike Microsoft Edge Chakra Engine InitClass Type Confusion	CWE: 119 CVE: 2019-0539 BID: 106401 EXPLOITDB : 46203 GOOGLE: 1703	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically a type confusion vulnerability exists inside the Chakra Javascript engine InitClass. It is possible for an attacker to craft javascript code in such a way that type confusion will cause a memory access violation to occur. This may lead to remote code execution or a denial of service condition in the browser.
Strike Windows mshtml Engine Remote Code Execution	CWE: 20 CVE: 2019-0541 EXPLOITDB : 46536 BID: 106402	This strike exploits a vulnerability in the Microsoft mshtml Engine. The vulnerability is due to improper filtering of the "edit" parameter. An attacker could exploit this vulnerability by enticing the victim to click a malicious link and download the malicious html file. Successful exploitation may lead to remote code execution on the client.
Strike Microsoft Edge Chakra NewScObjectNoCtor Type Confusion	CWE: 119 CVE: 2019-0567 EXPLOITDB : 46203 BID: 106418 GOOGLE: 1702	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that when using the NewScObjectNoCtor or InitProto methods with the SetIsPrototype method of the type handler, a transition to a new type can cause type confusion to occur. This can lead to a denial of service in the browser or potentially lead to remote code execution.
Strike Microsoft Edge Chakra JsBuiltInEngineInterfaceExtensionObject Use After Free	CWE: 119 CVE: 2019-0568 EXPLOITDB : 46205 BID: 106420 GOOGLE: 1709	This strike exploits a vulnerability in the Microsoft Edge browser. Specifically, the vulnerability exists in the Javascript Chakra engine. It is possible to craft Javascript in such a way that when using the InjectJsBuiltInLibraryCode method an attacker can clear the disable-implicit-call flag can lead to a stack based use after free condition. This may lead to a denial of service condition in the browser, or potentially remote code execution.

Name	References	Description
Strike Microsoft SharePoint DecodeEntityInstanc eid Insecure Deserialization	CWE: 20 CVE: 2019-0604	This strike exploits an insecure deserialization vulnerability in Microsoft SharePoint. The vulnerability is due to insufficient validation of user-supplied data to 'EntityInstanceIdEncoder' class. A remote, authenticated attacker could exploit this vulnerability by sending maliciously crafted HTTP requests to a target SharePoint server. Successful exploitation of this vulnerability leads to remote code execution on the target SharePoint web application.
Strike Microsoft Windows scripting engine code execution	CWE: 119 CVE: 2019-0752	This strike exploits a vulnerability in the Microsoft Windows scripting engine. The vulnerability is due to incorrect handling of objects in memory. An attacker could exploit this vulnerability by enticing a user to view a malicious web page. Successful exploitation of the vulnerability could trigger a code execution condition on client side.
Strike Microsoft Internet Explorer VBScript Execution Policy Bypass	CWE: 254 CVE: 2019-0768 GOOGLE: 1738	This strike exploits a vulnerability in Microsoft Internet Explorer. By utilizing VBScript.Encode it is possible to bypass the MSHTML Security Zone security policy that is put in place to allow or restrict VBScript from execution.
Strike Microsoft Windows ActiveX Data Objects Code Execution	CWE: 119 CVE: 2019-0888	A code execution vulnerability has been reported in Microsoft Windows ActiveX Data Objects (ADO). The vulnerability is due to improper handling of an object. A remote attacker could exploit this vulnerability by enticing a user to open a specially crafted file. Successful exploitation could result in the execution of arbitrary code with the victim's privileges.
Strike Jenkins Script Security Plugin Authenticated Remote Command Execution	CWE: 254 CVE: 2019-10030 00 BID: 106681	This strike exploits a remote command execution vulnerability in Script Security Plugin pertaining to Jenkins master. The vulnerability is due to improper validation of data passed to the Jenkins master sandbox. A specially crafted HTTP POST request containing a sandbox script leads to remote code execution conditions on the vulnerable server.
Strike Jenkins Script Security Plugin Sandbox Bypass Vulnerability	CWE: 20 CVE: 2019-10030 29	This strike exploits a sandbox bypass vulnerability in the Jenkins Script Security Plugin. The vulnerability is due to improper validation of data passed to the Jenkins sandbox. It leverages Groovy metaprogramming to download and execute a malicious JAR file. The security plugin fails to adequately restrict the execution of untrusted code, allowing remote, unauthenticated attackers with Overall/Read permission to bypass the security sandbox and run malicious scripts. Successful exploitation could result in remote code execution.

Name	References	Description
Strike Jenkins Groovy Plugin Authenticated Remote Command Execution	CWE: 20 CVE: 2019-10030 30	This strike exploits a sandbox bypass vulnerability in Script Security Plugin pertaining to Jenkins master. The vulnerability is due to improper validation of data passed to the Jenkins master sandbox. An attacker can exploit this flaw by sending a specially crafted HTTP POST request containing a sandbox script SecureGroovyScript/checkScript. Successful exploitation of the vulnerability can lead to remote code execution on the vulnerable server.
Strike Kentico Unauthenticated Remote Code Execution via Insecure Dot Net Deserialization	CVE: 2019-10068 CWE: 502	This strike exploits an insecure deserialization vulnerability in Kentico. The vulnerability arises due to a failure to validate security headers in the staging service allowing an attacker to bypass authentication and perform arbitrary operation. An unauthenticated remote attacker can trigger insecure deserialization of user-controlled .NET objects, by sending a specially crafted request, leading to remote code execution. A successful attack could result in full compromise of the Kentico instance and underlying server.
Strike XStream Library ReflectionConverter Insecure Deserialization	CWE: 502 CVE: 2019-10173	This strike exploits an insecure deserialization vulnerability in XStream Library. The vulnerability is due to insufficient validation of event handler type in user-supplied XML data. The issue arises from default configuration changes. When converting a 'dynamic-proxy' element to a Proxy instance, XStream generates a handler object based on the 'handler' element's class attribute. Of particular concern is the java.bean.EventHandler class, which, if exploited, allows an attacker to craft a malicious 'handler' element, potentially enabling the execution of arbitrary commands. A remote attacker could exploit this vulnerability by sending specially crafted XML file to the affected application. Successful exploitation could allow the attacker to execute arbitrary command under the security context of the process.
Strike Jenkins SCM Git Client Plugin Authenticated OS Command Injection	CWE: 78 CVE: 2019-10392	An OS command injection exists in Jenkins Git Client plugin. The vulnerability is due to lack of parameter sanitization while parsing parameters set to configure a Jenkins job. By exploiting this flaw, an authenticated remote attacker can run arbitrary OS commands on the target system. Note: All versions of Jenkins Git Client below 2.8.2 are affected by this vulnerability.
Strike Jenkins CI Server build-metrics Cross-Site Scripting	CWE: 79 CVE: 2019-10475	This strike exploits a cross-site scripting vulnerability has been reported in build-metrics plugin of Jenkins CI. This vulnerability is due to insufficient input validation of user supplied query string. A remote attacker could exploit this vulnerability by enticing the target to click on a crafted link. Successful exploitation could result in execution of script code in the security context of the target user's browser.
Strike Mongo Express VM Dependency Remote Command Execution	CWE: 94 CVE: 2019-10758	This strike exploits a remote code execution vulnerability in mongo-express. This vulnerability is triggered via endpoints that uses the toBSON method and misuses the vm dependency to perform exec commands in a non-safe environment. A remote, authenticated attacker could exploit this vulnerability by sending a request to a target server. Successfully exploiting this vulnerability could result in arbitrary code execution on the target system.

Name	References	Description
Strike Joomla Core Directory Traversal	CWE: 22 CVE: 2019-10945 EXPLOITDB : 46710	This strike exploits a directory traversal vulnerability in Joomla Core 1.5.0 - 3.9.4. The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this vulnerability by sending crafted HTTP traffic to the target server. Successful exploitation could lead to file access outside the media manager root directory.
Strike Lighttpd url-path-2f-decode Denial-of-Service	CWE: 190 CVE: 2019-11072 BID: 107907	This strike exploits an integer overflow vulnerability in Lighttpd. The vulnerability is due to url mishandling of /%2F? in burl.c under HTTP GET request. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation results in denial-of-service on the target server. *Note: The exploit will work only when the target server's configuration "url-path-2f-decode" is set to enable.
Strike RabbitMQ X-Reason HTTP Header Denial of Service	CWE: 400 CVE: 2019-11287	A denial-of-service flaw exists in Pivotal RabbitMQ, versions 3.7.x prior to 3.7.21 and 3.8.x prior to 3.8.1, and RabbitMQ for Pivotal Platform, 1.16.x versions prior to 1.16.7 and 1.17.x versions prior to 1.17.4. An authenticated attacker may crash the service by sending a crafted X-Reason HTTP header containing an Erlang format string which causes the server to allocate a massive memory region.
Strike Zoho ManageEngine Applications Manager FaultTemplateOptions.jsp resourceid SQL Injection	CWE: 89 CVE: 2019-11469 EXPLOITDB : 46740	This strike exploits an SQL injection vulnerability in Zoho ManageEngine Applications Manager. The vulnerability is caused by insufficient validation of user input "resourcetype" on HTTP requests which are used to create SQL queries. Successful exploitation could allow an attacker abilities to execute SQL queries on the target server.
Strike Pulse Connect Secure html5acc Arbitrary File Disclosure	CWE: 275 CVE: 2019-11510 BID: 108073	This strike simulates an attack on Pulse Connect Secure versions prior to 8.1R15.1, 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4. The flaw takes advantage of a directory traversal vulnerability and allows remote unauthenticated attackers to read arbitrary files residing on the host system.
Strike Atlassian Crowd and Crowd Data Center Arbitrary Plugin Install RCE	CWE: 732 CVE: 2019-11580	This strike exploits a vulnerability in Atlassian Crowd and Crowd Data Center due to the pdkinstall development plugin incorrectly enabled in release builds. Attackers who can send unauthenticated or authenticated requests to a Crowd or Crowd Data Center instance can exploit this vulnerability to install arbitrary plugins, which permit remote code execution on systems running a vulnerable version of the application.
Strike Atlassian JIRA Template Injection Code Execution	CWE: 94 CVE: 2019-11581	This strike exploits a remote code execution in the JIRA Template. The vulnerability is due to improper sanitization of user input which is passed to the application via the ContactAdministrators and SendBulkMail actions. A remote authorized attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation results in remote code execution on the target server.

Name	References	Description
Strike HPE Intelligent Management Center IccSelectDevTypeBean Expression Language Inject	CWE: 287 CVE: 2019-11941	This strike exploits an expression language injection vulnerability in the HPE Intelligent Management. The vulnerability is due to improper sanitization of user input "beanName" which is passed to the application via the IccSelectDevTypeBean class. A remote authorized attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation results in remote code execution on the target server with SYSTEM privilege.
Strike Internet Explorer Scripting Engine Memory Corruption	CWE: 119 CVE: 2019-1221	This strike exploits a memory corruption vulnerability in Internet Explorer. The vulnerability is due to improper handling of memory objects. By enticing a user to access a specially crafted page, an attacker could exploit this vulnerability to corrupt memory and remotely execute malicious code in the context of the current user.
Strike GrandNode Ecommerce LetsEncryptController Directory Traversal	CWE: 22 CVE: 2019-12276	This strike exploits a directory traversal vulnerability in GrandNode Ecommerce platform. The vulnerability is due to improper sanitization of parameters passed to the "LetsEncryptController" module. By successfully exploiting this vulnerability, a remote, unauthenticated attacker could retrieve arbitrary files from the target server.
Strike Viber for Desktop Uri Handler Remote Code Execution	CWE: 426 CVE: 2019-12569	This strike exploits a remote code execution on the Viber Desktop. The vulnerability is due to improper sanitization of user input which is passed to the application via the DLL loading path. A remote unauthorized attacker can exploit this vulnerability by enticing the victim to open a crafted web page. Successful exploitation results in remote code execution on the victim's application.
Strike Cisco IOS XE WebUI snortcheck.lua Authenticated Command Injection	CWE: 78 CVE: 2019-12650	This strike exploits a command injection vulnerability in the WebUI component of Cisco IOS XE. The vulnerability is due to improper validation of user-supplied 'snortcheck.lua' form data via the WebUI. A user with low privilege access can exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation results in execution of Cisco console commands with administrative privileges.
Strike Cisco IOS XE WebUI Authenticated Command Injection	CWE: 78 CVE: 2019-12651	This strike exploits a command injection vulnerability in the WebUI component of Cisco IOS XE. The vulnerability is due to improper validation of user-supplied form data via the WebUI. A user with low privilege access can exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation results in the execution of Cisco console commands with administrative privileges.
Strike phpMyAdmin Setup Server Removal Cross-Site Request Forgery	CWE: 352 CVE: 2019-12922	This strike simulates a CSRF attack on phpMyAdmin. The flaw is a result of no anti-CSRF technique being employed in the setup page. A remote attacker may entice a phpMyAdmin user to make a request to a crafted URL, leading to removal of arbitrary servers from the phpMyAdmin configuration.
Strike Citrix SD WAN SQL Injection	CWE: 89 CVE: 2019-12989	This strike exploits an SQL Injection vulnerability in Citrix SD-WAN. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted http requests containing shell metacharacters in sitename parameter to get_package_file endpoint. Successful exploitation could allow the attacker to achieve remote code execution.

Name	References	Description
Strike Centreon nagios path OS Command Injection	CWE: 77 CVE: 2019-13024 EXPLOITDB : 47069	An OS command injection exists in Centreon 19.04.0 due to lack of sanitization when the 'nagios' binary path is set. By exploiting this flaw, an authenticated remote attacker can run arbitrary OS commands on the target system.
Strike SolarWinds Serv-U FTP Server USER_FULL_NAME Stored Cross-Site Scripting	CWE: 79 CVE: 2019-13182	This strike exploits a stored cross-site scripting vulnerability in the SolarWinds Serv-U FTP Server. The vulnerability is due to incorrect input validation prior to using the %USER_FULL_NAME% macro to render the Web UI. A remote, authenticated attacker could exploit this vulnerability by embedding malicious script code. A successful attack may result in the execution of script code in the security context of the target user.
Strike Wordpress Plugin Like Button Authentication Bypass	CWE: 287 CVE: 2019-13344 EXPLOITDB : 47078	This strike exploits an authentication bypass on the Wordpress Plugin Like Button. The vulnerability is due to not properly checking if the request is sent by an authorized user. A remote unauthorized attacker can exploit this vulnerability by sending a crafted HTTP POST request to the system. Successful exploitation results in changing the configuration of the plugin setting.
Strike D-Link Central WiFi Manager CWM(100) IndexAction Remote Code Execution	CVE: 2019-13372 CWE: 94	A remote code execution vulnerability exists in D-Link Central WiFi Manager CWM(100) due to lack of user-supplied data sanitization. The vulnerable code resides in '/web/Lib/Action/IndexAction.class.php' source and uses the HTTP 'Cookie' header value to construct a string which is later evaluated as PHP code. By sending a crafted HTTP POST request, a remote unauthenticated attacker may run arbitrary PHP code as the SYSTEM user.
Strike D-Link Central WiFi Manager CWM(100) dbSQL SQL Injection	CVE: 2019-13373	A SQL injection vulnerability exists in D-Link Central WiFi Manager CWM(100) due to lack of user request authorization. The vulnerable code resides in '/web/Public/Conn.php' source and uses the HTTP 'dbSQL' parameter value to perform database lookups. By sending a crafted HTTP POST request, a remote unauthenticated attacker may gain access to the platform by adding user accounts or read existing data from the database.
Strike Microsoft Windows Jet Database Out of Bounds Write	CWE: 119 CVE: 2019-1359	This strike exploits an Out of Bounds Write vulnerability in Microsoft Jet Database Engine. The vulnerability is due to improper handling of objects in memory. The user would be enticed to visit a site or open a web page, causing arbitrary code to be executed.
Strike Google Chrome DesktopMediaPickerController WebContentsDestroyed Use After Free	CVE: 2019-13767 GOOGLE: 1985	This strike exploits a vulnerability in Google Chrome. An attacker can utilize the desktopCapture.chooseDesktopMedia API to trigger the WebContentsDestroyed method on a freed object causing a use after free condition to occur. This can result in a denial of service condition in the browser or potentially remote code execution.

Name	References	Description
Strike Django Json-Hstore Field SQL Injection	CWE: 89 CVE: 2019-14234	This strike exploits a SQL injection vulnerability in the Django server. The vulnerability is caused by insufficient validation of user input on HTTP requests, which are used to create SQL queries. Successful exploitation could allow an attacker to execute SQL command on the target server.
Strike HAProxy cookie Denial-of-Service	CWE: 20 CVE: 2019-14241 BID: 109352	This strike exploits a denial of service vulnerability in HAProxy server. The vulnerability is due to incorrect handling of the cookie header under HTTP traffic. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation results in denial-of-service on the target server.
Strike Microsoft Internet Explorer toJSON callback Use-After-Free	CWE: 119 CVE: 2019-1429	This strike exploits a vulnerability in the Microsoft Internet Explorer scripting engine. Specifically, an attacker can craft an HTML page containing a Javascript script in such a way that a call to 'jscript!JSONStringifyObject()' frees an object that is later going to be referred by 'jscript!PrepareInvoke()', resulting in a use-after-free condition. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Strike Wordpress Plugin UserPro Reflected Cross-Site Scripting	CWE: 79 CVE: 2019-14470 EXPLOITDB : 47304	This strike exploits a cross-site scripting vulnerability in Wordpress Plugin UserPro. This vulnerability is due to inadequate input filtering of "error_description" in the web interface. An attacker could exploit this vulnerability by enticing a user to visit an attacker controlled webpage or click a malicious link. By exploiting this vulnerability an attacker could trigger reflected cross site scripting on the victim's browser.
Strike OpenEMR ajax_download.php Directory Traversal Vulnerability	CVE: 2019-14530	This strike exploits a directory traversal vulnerability in OpenEMR. The vulnerability is located in the ajax_download.php script, specifically in the improper validation of the fileName parameter. Exploiting this vulnerability allows a remote, authenticated attacker to read or delete arbitrary files on the server, potentially leading to information disclosure or denial-of-service conditions.
Strike FusionPBX service_edit.php Authenticated OS Command Injection	CWE: 77 CVE: 2019-15029	An OS command injection exists in FusionPBX 4.4.8 due to lack of parameter sanitization while parsing requests to 'service_edit.php'. By exploiting this flaw, an authenticated remote attacker can run arbitrary OS commands on the target system.
Strike Webmin password_change.cgi Unauthenticated Remote Command Execution	CWE: 77 CVE: 2019-15107 EXPLOITDB : 47293	An OS command injection vulnerability exists in Webmin 1.920 and prior versions. The flaw exists in the password change functionality and is reachable via the '/password_change.cgi' endpoint. By exploiting this vulnerability, a remote unauthenticated attacker may execute arbitrary OS commands on the target system.

Name	References	Description
Strike Palo Alto GlobalProtect sslmgr Remote Code Execution	CWE: 20 CVE: 2019-1579	This strike exploits a format string vulnerability on Palo Alto GlobalProtect server. The flaw resides in the 'sslmgr' endpoint due to lack of user input validation. A remote unauthenticated attacker may thus crash a vulnerable instance or even execute arbitrary code.
Strike Cisco DCNM SecurityManager Hard-Coded Cryptographic Key Authentication Bypass	CVE: 2019-15976	This strike exploits an authentication bypass vulnerability in Cisco Data Center Network Manager. The vulnerability exists due to the use of a hard-coded cryptographic key shared across installations for validating Single Sign-On (SSO) tokens. A remote, unauthenticated attacker could exploit this vulnerability by crafting a valid SSO token, allowing them to bypass authentication and execute arbitrary actions through the SOAP API with administrative privileges.
Strike Cisco Data Center Network Manager saveZoneInputFileTo Server Directory Traversal	CWE: 22 CVE: 2019-15980	This strike exploits a directory traversal vulnerability in Cisco Data Center Network Manager. The vulnerability is due to insufficient validation of 'filename' HTTP parameter in the 'saveZoneInputFileToServer' method. An authenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation results in arbitrary file write, which can be used to achieve remote code execution with SYSTEM privileges.
Strike Cisco Data Center Network Manager getConfigTemplateFile Name SQL Injection	CWE: 89 CVE: 2019-15984	This strike exploits a SQL injection vulnerability in Cisco Data Center Network Manager. The vulnerability is due to insufficient input validation when processing HTTP requests within the 'getConfigTemplateFileName' method pertaining to the 'ConfigTemplateHandler' Java class. An authenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation could result in the code execution under the security context of the database process.
Strike D-Link DNS-320 ShareCenter Unauthenticated Remote Code Execution	CWE: 78 CVE: 2019-16057	An OS command injection vulnerability exists in D-Link DNS-320 ShareCenter versions <= 2.05.B10. The flaw is a result of no input sanitization on the 'port' parameter 'login_mgr.cgi' cgi requests. A remote unauthenticated attacker may issue system commands with 'root' privileges.
Strike Harbor Project Harbor user API Privilege Escalation	CWE: 862 CVE: 2019-16097	This strike exploits a privilege escalation vulnerability in Harbor. The vulnerability is due to insufficient validation of HTTP requests to the users API. The Post() function in user.go decodes JSON data from the request body which checks for the existence of a user, and creates a new user if necessary. If the JSON payload contains the "has_admin_role" key set to "true", the resulting user account is granted admin privileges. A remote attacker could exploit this vulnerability by sending an API request with a crafted JSON payload. Successful exploitation of this vulnerability could allow the attacker to create users with admin privileges.
Strike YouPHPTube checkConfiguration.php Remote Code Execution	CWE: 862 CVE: 2019-16124	This strike exploits an access control vulnerability in the checkConfiguration.php script of YouPHPTube. The vulnerability is due to a failure on part of the script to properly validate user requests. A remote attacker with knowledge of the database credentials could exploit this vulnerability by sending a crafted request to checkConfiguration.php and then subsequently browsing to the homepage. Successful exploitation allows the attacker to execute arbitrary code under the context of the server.

Name	References	Description
Strike Cisco Prime Data Center Network Manager Arbitrary File Upload	CWE: 264 CVE: 2019-1620 BID: 108906 EXPLOITDB : 47016	This strike exploits a path traversal vulnerability found in Cisco Data Center Network Manager (DCNM). The vulnerability is due to incorrect permission settings in affected DCNM software. An unauthenticated attacker could exploit this vulnerability by uploading a malicious file to the administrative web interface. A successful exploit could allow the attacker to write arbitrary files on the filesystem and execute code with root privileges on the affected device.
Strike Nostromo nhttpd http_verify Directory Traversal	CVE: 2019-16278 CWE: 22	This strike exploits a directory traversal vulnerability in Nostromo nhttpd server. The vulnerability is due to a failure on part of the <code>http_verify</code> function to properly parse user requests. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation could result in information disclosure and in the worst case, allows the attacker to execute arbitrary system commands under the context of the server process.
Strike Cisco Small Business authenticated Command Injection	CWE: 20 CVE: 2019-1652 BID: 106728 EXPLOITDB : 46243	This strike exploits a OS command injection vulnerability found in Cisco Small Business RV320 and RV325 routers. The vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by crafting a special HTTP POST request. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux shell as root.
Strike Cisco Small Business Unauthenticated Information Disclosure	CWE: 284 CVE: 2019-1653 BID: 106732 EXPLOITDB : 46262	This strike exploits a information disclosure vulnerability found in Cisco Small Business RV320 and RV325 routers. The vulnerability is due to improper access controls for URLs. An attacker could exploit this vulnerability by connecting to an affected device via HTTP or HTTPS and requesting specific URLs. A successful exploit could allow the attacker to download the router configuration or detailed diagnostic information.
Strike rConfig ajaxServerSettingsChk Command Injection	CWE: 78 CVE: 2019-16662	A command injection vulnerability exists in the rConfig network device configuration management tool. The vulnerability is due to insufficient input validation in the 'ajaxServerSettingsChk.php' module. A remote, unauthenticated attacker can create a malicious HTTP request resulting in arbitrary command execution on the target system with the privileges of the user running the web server.
Strike vBulletin widget_php Remote Code Execution	CWE: 20 CVE: 2019-16759	A server-side template injection vulnerability that leads to remote code execution exists in vBulletin versions 5.0.0 up to 5.5.4. By exploiting it, a remote unauthenticated attacker may execute arbitrary code using server's PHP engine.

Name	References	Description
Strike WiKID 2FA Enterprise Server SQL Injection in searchDevices.jsp	CVE: 2019-16917	This strike exploits an SQL injection vulnerability in WiKID 2FA Enterprise Server. The vulnerability exists due to improper sanitization of user-supplied input in the searchDevices.jsp file. A remote, authenticated attacker could leverage this flaw by sending specially crafted HTTP requests, potentially leading to the execution of arbitrary SQL commands on the backend database.
Strike OpenProject sortBy query Reflected Cross Site Scripting	CWE: 79 CVE: 2019-17092	This strike exploits a reflected cross-site scripting vulnerability found in OpenProject Web interface. This vulnerability is due to inadequate input filtering in the web interface, while parsing input passed to 'sortBy' parameter within 'projects' page. By exploiting this vulnerability an attacker could cause arbitrary HTML/script code to be executed by the target user's browser.
Strike WiKID 2FA Enterprise Server processPref.jsp SQL Injection Vulnerability	CVE: 2019-17117	This strike exploits an SQL injection vulnerability in WiKID 2FA Enterprise Server. The vulnerability exists due to improper sanitization of user-supplied input in the processPref.jsp file. A remote, authenticated attacker can leverage this flaw by sending specially crafted HTTP requests, potentially leading to the execution of arbitrary SQL commands on the backend database.
Strike Zoho ManageEngine OpManager OPMDeviceDetailsServlet SQL Injection	CWE: 89 CVE: 2019-17602	This strike exploits an SQL injection vulnerability in Zoho ManageEngine OpManager. The vulnerability is caused by insufficient validation of parameter category. Successful exploitation could allow an attacker abilities to execute SQL queries on the target server.
Strike Cisco Prime Infrastructure EPNM XmpLogFilesDownloadServlet Directory Traversal	BID: 108351 CWE: 22 CVE: 2019-1819	This strike exploits a directory traversal vulnerability in Cisco Prime Infrastructure EP NM. The vulnerability is due to improper sanitization of the "downloadDirectory" parameter. By successfully exploiting this vulnerability, a remote, unauthenticated attacker could retrieve arbitrary files from the target server.
Strike Cisco Prime Infrastructure Health Monitor - TarArchive Directory Traversal	CWE: 20 CVE: 2019-1821 BID: 108339 EXPLOITDB : 47016	This strike exploits a path traversal vulnerability found in Cisco Prime Infrastructure (PI) and Cisco Evolved Programmable Network (EPN) Manager. The vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by uploading a malicious file to the administrative web interface. A successful exploit could allow the attacker to execute code with root-level privileges on the underlying operating system.
Strike Cisco Elastic Services Controller RESR API Authentication Bypass	CWE: 287 CVE: 2019-1867 BID: 108184	This strike exploits an authentication bypass vulnerability in the Cisco Elastic Services Controller. The vulnerability is due to improper filtering of the "Authorization" header. An attacker could exploit this vulnerability by sending a crafted http traffic to the target server. By successfully exploiting this vulnerability, a remote, unauthenticated attacker could achieve authentication bypass on the target server.

Name	References	Description
Strike rConfig HTTP ajaxArchiveFiles OS Command Injection	CWE: 78 CVE: 2019-19509	An OS Command Injection exists in rConfig 3.9.3 and prior versions as a result of no sanitization of user supplied data. The parameter processed in 'ajaxArchiveFiles.php' is then used as a command line argument within a privileged command. By sending a crafted 'path' parameter to '/lib/ajaxHandlers/ajaxArchiveFiles.php' path, a remote authenticated attacker may execute arbitrary OS commands as a superuser.
Strike Citrix Application Delivery Controller Command Injection via vpn Directory Traversal	CWE: 22 CVE: 2019-19781	An OS command injection vulnerability exists in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. The command injection is possible using a directory traversal flaw, due to improper sanitization of multiple fields in HTTP requests. The flaw may be exploited by an unauthenticated attacker to execute arbitrary commands on the target server.
Strike Oracle Java Arbitrary File Deletion	CWE: 284 CVE: 2019-2449 BID: 106597	This strike exploits an arbitrary file deletion vulnerability in Oracle SE 8. The vulnerability is due to improper filtering of jlnp URL variable. An attacker can entice the victim to click the malicious link. Successful exploitation may lead to file deletion on client side.
Strike Oracle WebLogic Server FileDistributionServlet Information Disclosure	CWE: 22 CVE: 2019-2615	The strike exploits a directory traversal vulnerability in Oracle WebLogic Server. The vulnerability arises from inadequate validation of the adminPath, file_name, and wl_managed_server_independence_request_filename headers associated with the file download feature in the WebLogic server, provided by the bea_wls_management_internal2.war application. An authenticated remote attacker could exploit this vulnerability by specifying relative or absolute path HTTP GET request headers. Successful exploitation leads to the disclosure of arbitrary file contents within the target system.
Strike Oracle Weblogic DeploymentService Arbitrary File Upload RCE	CWE: 284 CVE: 2019-2618	This strike simulates an arbitrary file upload attack on Oracle Weblogic. The vulnerability is a result of no sanitization for the 'wl_upload_application_name' header. Successful exploitation requires valid credentials and leads to arbitrary file upload and remote code execution.
Strike Oracle E-Business Suite General Ledger SQL Injection	CWE: 284 CVE: 2019-2638	A SQL injection vulnerability exists in the 'General Ledger' component of Oracle E-Business Suite. A SQL query may be sent via the 'Thin Client Framework' protocol over HTTP, which is later processed in the 'DataManagerServer.readSynch()' method located in 'oracle/apps/gl/jahe/tcf/server/DataManagerServer.java'. The string is then used as a base string for a database query. By exploiting this flaw, a remote unauthenticated attacker may execute arbitrary database queries.

Name	References	Description
Strike Oracle Weblogic Server AsyncResponseService Deserialization Remote Code Execution	CWE: 284 CVE: 2019-2725 BID: 108074 EXPLOITDB : 46780	This strike simulates a remote code execution attack on a Oracle Weblogic Server. The flaw is due to no authentication and no client input sanitization on server when receiving SOAP calls. By exploiting a vulnerable system, a remote unauthenticated attacker is able to execute arbitrary commands on the target system.
Strike Oracle Weblogic Server CoordinatorPortType Deserialization Remote Code Execution	CWE: 284 CVE: 2019-2729	This strike simulates a remote code execution attack on Oracle Weblogic Server. The flaw is due to lack of authentication and input sanitization when the server receives SOAP calls. By exploiting a vulnerable system, a remote unauthenticated attacker is able to execute arbitrary commands on the target system.
Strike Atlassian Confluence Server file inclusion	CWE: 22 CVE: 2019-3396 BID: 107543	This strike exploits a file inclusion and remote command execution vulnerability in Atlassian Confluence Server. The vulnerability is due to improper sanitization of the "_template" parameter. By successfully exploiting this vulnerability, a remote, unauthenticated attacker could retrieve arbitrary files from the target server and achieve file inclusion or achieve remote command execution by SSTI, inject malicious template and have it executed.
Strike Atlassian Confluence Download Attachments Remote Code Execution	CWE: 22 CVE: 2019-3398	This strike exploits a path traversal vulnerability in the downloadallattachments resource of Confluence Server and Data Center. The vulnerability is due to improper validation of parameters in a HTTP POST request. To exploit this vulnerability, a remote, authenticated attacker who has the permission to add attachments to pages or blogs can upload a file with directory traversal characters in its name. After that, when Download All functionality is used, it copies the file at the traversed location. A successful attack may result in arbitrary command execution in the context of the server process. Note: The JSESSIONID cookie and CSRF token are acquired during authentication (not shown).
Strike OpenEMR download_template.php Directory Traversal	CWE: 22 CVE: 2019-3967	This strike exploits a directory traversal vulnerability in OpenEMR. The vulnerability is due to improper sanitization of the "form_filename" parameter. By successfully exploiting this vulnerability, a remote, unauthenticated attacker could retrieve arbitrary files from the target server.
Strike OpenEMR scanned_notes-new.php OS Command Injection	CWE: 77 CVE: 2019-3968	A command injection vulnerability exists in OpenEMR 5.0.1 and earlier, within 'scanned_notes/new.php' form file, as a result of weak user input sanitization. By sending a crafted 'id' parameter in a HTTP request, a remote authenticated attacker might execute arbitrary system commands.
Strike Exhibitor UI Command Injection	CWE: 78 CVE: 2019-5029	This strike exploits a command injection vulnerability in the Exhibitor Web UI. The vulnerability is due to improper parsing of parameters passed to the config editor web form. A malicious attacker can exploit this by performing a specially-crafted HTTP request. Successful exploitation leads to arbitrary commands being run in the context of the user running the Exhibitor server.

Name	References	Description
Strike HPE IMC Expression Language Injection via beanName Parameter	CVE: 2019-5373	This strike exploits an Expression Language injection vulnerability in HPE Intelligent Management Center. The vulnerability exists due to improper validation of the `beanName` parameter in the `CustomReportTemplateSelectBean` class. A remote, authenticated attacker can leverage this flaw to execute arbitrary code on the target system with SYSTEM-level privileges.
Strike HPE Intelligent Management Center Expression Language Injection Vulnerability cve_2019_5385	CVE: 2019-5385	This strike exploits an Expression Language injection vulnerability in HPE Intelligent Management Center. The vulnerability resides in the insufficient validation of the beanName parameter within the perfSelectTask endpoint. Exploiting this flaw allows a remote attacker to execute arbitrary code on the target system under the security context of the SYSTEM user.
Strike HPE Intelligent Management Center ViewBatchTaskResultDetailBean Expression Language Injection	CWE: 74 CVE: 2019-5386	This strike exploits a remote code execution in the HPE Intelligent Management Center. The vulnerability is due to improper sanitization of user input "beanName" which is passed to the application via the ViewBatchTaskResultDetailBean class. A remote authorized attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation results in remote code execution on the target server with SYSTEM privilege.
Strike Ruby on Rails template_renderer Accept Header File Disclosure	CWE: 200 CVE: 2019-5418	The strike replicates an attack on Ruby on Rails which leads to arbitrary file disclosure. The vulnerability resides in the lack of validation of the "Accept" header which is further parsed within the "template_renderer.rb" file in order to return the template file to be rendered. By exploiting this, a remote unauthenticated attacker may read arbitrary files on the host system.
Strike Ruby on Rails Token Disclosure Active Storage RCE	CWE: 20 CVE: 2019-5420 EXPLOITDB : 46785	This strike replicates a remote code execution attack on Ruby on Rails (<5.2.2.1, <6.0.0.beta3). The flaw resides in the deterministic way the platform generates its secret token in development mode, making it easy to be guessed. A successful exploitation results in arbitrary code execution through Marshal object injection.
Strike Chrome browser FileReader API use after free	CWE: 416 CVE: 2019-5786	This strike replicates a use-after-free exploit for Chromium browser engine. The vulnerability can be triggered via the FileReader JS API by creating two array references to the same file reader result then using another mechanism to free the underlying memory. By successfully exploiting this flaw, an attacker can execute arbitrary code in the context of the Chrome's 'renderer' process.
Strike Drupal Core Phar Stream Insecure PHP Deserialization	CWE: 20 CVE: 2019-6339	A remote code execution vulnerability exists in Drupal 7.x before 7.62, Drupal 8.5.x before 8.5.9 and Drupal 8.6.x before 8.6.6. The vulnerability is located within the PHP's built-in phar stream wrapper, when performing file operations on an untrusted 'phar://' URI. A remote attacker can exploit this vulnerability by sending a crafted HTTP packet to the target service. Successful exploitation could lead to arbitrary code execution or crash of the vulnerable application.

Name	References	Description
Strike Drupal REST API PHP deserialization Remote Code Execution	CWE: 20 CVE: 2019-6340 BID: 107106	A remote code execution vulnerability exists in Drupal 8.5.x before 8.5.11 and Drupal 8.6.x before 8.6.10. The vulnerability is due to the lack of data sanitization originating from non-form sources in the REST module. A remote attacker can exploit this vulnerability by sending a crafted HTTP packet to the target service. Successful exploitation could lead to arbitrary code execution or crash of the vulnerable application.
Strike ES File Explorer File Manager Policy Bypass	CWE: 306 CVE: 2019-6447	This strike exploits a policy bypass vulnerability in the android app ES File Explorer File Manager. The vulnerability is due to misconfigured access control of a web server listening for commands. A remote, unauthenticated attacker could exploit this vulnerability by sending a malicious request to an Android device running a vulnerable version of the product. Successful exploitation of this vulnerability could allow the attacker to download then launch applications as well as read arbitrary files. *NOTE: In OneArm mode, the strike will try to perform one of the following actions depending on the variant ran - open the settings app or list Files or download the /system/bin/cp binary present on the victim android device.
Strike QNAP Photo Station Improper Access Control Vulnerability	CVE: 2019-7192 CWE: 863	This strike exploits an improper access control vulnerability in Qnap Photostation. The vulnerability exists due to insufficient validation of user-supplied parameters in backend API endpoints. An unauthenticated attacker with network access to the affected QNAP NAS can exploit this issue by sending crafted requests to specific Photo Station APIs, which may result in unauthorized access to system files.
Strike Nexus Repository Manager 3 Remote Code Execution	CWE: 284 CVE: 2019-7238	This strike exploits a remote code execution on Nexus Repository Manager 3. This vulnerability is due to improper handling of the "value" parameter under HTTP parameter when a client sends http traffic to the server. A remote unauthenticated attacker can exploit this vulnerability by sending crafted http requests to the target server. Successful exploitation results in remote code execution.
Strike Nice Linear eMerge E3-Series OS Command Injection Vulnerability	CWE: 78 CVE: 2019-7256	This strike exploits a command injection vulnerability in Linear eMerge E3-Series. The vulnerability is due to insufficient sanitizing of user supplied inputs. With port 80 exposed to the internet for remote management, an unauthenticated attacker could exploit this vulnerability. The attacker gains complete control over critical infrastructure, potentially using compromised devices in distributed denial-of-service attacks.
Strike SonicWall SMA100 SQL Injection Vulnerability	CWE: 89 CVE: 2019-7481	This strike exploits SQL injection vulnerability in SonicWall SMA100. The vulnerability is due to improper neutralization of special elements used in SQL command. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary SQL commands, potentially leading to unauthorized access
Strike Elastic Kibana Timelion Prototype Pollution Remote Code Execution	CWE: 77 CVE: 2019-7609	This strike replicates a remote code execution attack on Elastic Kibana, through a JavaScript prototype pollution vector. The vulnerability is due to lack of sanitization for user supplied data when parsing Timelion component requests. By exploiting this flaw, a remote unauthenticated attacker might execute arbitrary code on the target system.

Name	References	Description
Strike Adobe Coldfusion CFFILE File Upload	CWE: 434 CVE: 2019-7838	This strike exploits a file upload vulnerability in Adobe Coldfusion. The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this vulnerability by sending crafted HTTP traffic to the target server. Successful exploitation could lead to file upload and code execution on the target server.
Strike Zoho ManageEngine ServiceDesk Plus Arbitrary File Upload	CWE: 434 CVE: 2019-8394 EXPLOITDB : 46413	This strike exploits a file upload vulnerability in Zoho ManageEngine ServiceDesk Plus. Files can be uploaded to the target by sending an HTTP POST request with a parameter 'module' equal to 'CustomLogin'. An attacker can send a malicious HTTP POST request to upload an arbitrary file to '/custom/login' folder. Successful exploitation may lead to creation and execution of arbitrary files by an authenticated user with minimum permissions (for example, guest).
Strike Apple Safari Webkit AIR Dangling Pointer Register	CWE: 119 CVE: 2019-8611 GOOGLE: 1788	This strike exploits a vulnerability in Apple Safari Webkit. Specifically after optimizations are performed on AIR code, a register gets marked as late use and ultimately is determined to be a dead register and discarded. It may be possible for an attacker to construct Javascript in such a way that it is possible to control the data in this dangling register. This can cause a denial of service condition in the browser or potentially allow for remote code execution to occur.
Strike Apple Safari Webkit ValueProfiles Use After Free	CWE: 119 CVE: 2019-8672 GOOGLE: 1825	This strike exploits a vulnerability in Apple Safari Webkit. Specifically a JSValue ValueProfile pointing to a previously freed chunk of memory which will have its JSCell header overwritten. When this gets accessed out of bounds a crash will occur. An attacker can craft javascript in such a manner that will cause memory corruption to occur, causing a denial of service in the browser and potentially leading to remote code execution.
Strike Apple Safari Webkit emitEqualityOpImpl Wrongly Replaced Method	CWE: 119 CVE: 2019-8684 GOOGLE: 1850	This strike exploits a vulnerability in Apple Safari Webkit. It is possible for an attacker to construct Javascript in such a way that when the emitEqualityOpImpl method is called it will incorrectly replace the typeof instruction with the is_cell_with_type instruction. This can cause a denial of service condition in the browser or potentially allow for remote code execution to occur.
Strike Apple Safari Webkit ArgumentsEliminationPhase Uninitialized Variable Access	CWE: 119 CVE: 2019-8689 GOOGLE: 1876	This strike exploits a vulnerability in Apple Safari Webkit. Specifically when trying to inline GetByVal operations on stack-allocated arguments the code fails to properly check whether index is lower than numberOfArgumentsToSkip. This can potentially lead to uninitialized variable access which can cause a denial of service condition in the browser or allow for remote code execution to occur.

Name	References	Description
Strike WordPress Core wp_crop_image Local File Inclusion Remote Code Execution	CWE: 94 CVE: 2019-8942 BID: 107088 EXPLOITDB : 46511	The strike exploits a local file inclusion vulnerability in WordPress platform, leveraged beforehand by a path traversal via the 'wp_attached_file' parameter. By supplying a 'wp_page_template' metadata parameter, the attacker determines the theme engine to include a malicious uploaded file. By exploiting this vulnerability an authenticated attacker gains remote code execution on the target host system.
Strike WordPress Core _wp_attached_file Post Edit Directory Traversal	CWE: 22 CVE: 2019-8943 BID: 107089 EXPLOITDB : 46511	The strike emulates a path traversal attack on WordPress CMS platform. The attack can be carried by a low privileged user by providing a '_wp_attached_file' parameter when editing media files, thus modifying post metadata. By leveraging this vulnerability with a local file inclusion exploit, an attacker may gain code execution on the host system.
Strike ThinkPHP 5.x Remote Code Execution	CWE: 20 CVE: 2019-9082 EXPLOITDB : 45978 EXPLOITDB : 46150	This strike exploits a remote command execution vulnerability in ThinkPHP 5.x less than v5.0.23, v5.1.31. The vulnerability is due to improper validation of parameters in a HTTP GET request. A remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the server. A successful attack may result in arbitrary command execution in the context of the server process.
Strike Joomla component J2Store SQL Injection	EXPLOITDB : 46467 CWE: 89 CVE: 2019-9184	This strike exploits a SQL injection vulnerability in the J2Store component 3.x - 3.3.6 for Joomla!. The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this vulnerability by sending specifically crafted packets, potentially resulting in the execution of SQL commands which may lead to information disclosure.
Strike WordPress Plugin Localize 1.0 Local File Inclusion	EXPLOITDB : 46537 CWE: 77 CVE: 2019-9618	This strike exploits a remote file inclusion vulnerability in WordPress Plugin Grace. The vulnerability is due to improper sanitization of the "cfg" parameter. By successfully exploiting this vulnerability, a remote, unauthenticated attacker could retrieve arbitrary files from the target server.

Name	References	Description
Strike Synacor Zimbra Collaboration Suite Mailboxd Component XXE Vulnerability	CVE: 2019-9670 CWE: 611	This strike exploits an XXE vulnerability in Synacor Zimbra Collaboration Suite. This vulnerability lies in the Mailboxd component. A remote unauthenticated attacker can exploit this vulnerability by crafting a specially crafted XML payload containing malicious code and targeting the Autodiscover/Autodiscover.xml endpoint. Successful exploitation of this vulnerability could lead to data exposure.
Strike Symantec DLP ProtectManager Persistent XSS	CWE: 79 CVE: 2019-9701 EXPLOITDB : 47071	This strike simulates a stored XSS attack on Symantec DLP 15.5 MP1. The flaw exists in '/ProtectManager/enforce/admin/senderrrecipientpatterns/list' endpoint due to lack of sanitization for the 'name' parameter. A successful authenticated attacker is thus able gain control of victim's browser.
Strike WordPress Comment Content Filter Remote Code Execution	CVE: 2019-9787 CWE: 352	This strike exploits a remote code execution vulnerability in WordPress. The vulnerability is due to lack of protection against cross-site request forgery attack and improper validation of the comment content in the wp_rel_nofollow_callback function which leads to stored cross-site scripting issue. A remote, unauthenticated attacker could exploit this vulnerability by enticing an authenticated user to open a web page or link. Successful exploitation, in the worst case, could lead to execution of arbitrary PHP code. *NOTE - In this strike we are just covering the initial stages of exploitation where the attacker serves the website with the malicious link
Strike Mozilla Firefox IonMonkey MArraySlice Out of Bounds Write	CWE: 119 CVE: 2019-9810	This strike exploits a vulnerability in Spidermonkey, the Javascript engine of Mozilla Firefox. The issue is caused by incorrect alias information for Array.prototype.slice method within IonMonkey JIT compiler component. This can lead to a denial of service or potentially allow for remote code execution to occur.
Strike Mozilla Firefox Spidermonkey IonMonkey ObjectGroup Type Confusion	CWE: 704 CVE: 2019-9816 GOOGLE: 1808	This strike exploits a vulnerability in Mozilla Firefox. Specifically, the vulnerability exists in the Javascript engine Spidermonkey. It is possible to craft Javascript in such a way that in IonMonkey an unexpected ObjectGroup in an ObjectGroupDispatch operation might allow for unsafe code to execute. This could cause type confusion to occur causing a denial of service condition in the browser or potentially allowing for remote code execution to occur.
Strike WordPress Social Warfare Plugin Authenticated Remote Command Execution	CWE: 79 CVE: 2019-9978	This strike exploits a design weakness in the WordPress plugin Social Warfare, stemming from insufficient input validation and sanitization. A remote unauthenticated attacker could exploit this vulnerability by sending a specially crafted request to the server. Successful exploitation could result in remote code execution, allowing the attacker to execute arbitrary code on the affected server.

Name	References	Description
Strike Microsoft SQL Server Reporting Services Remote Code Execution	CWE: 502 CVE: 2020-0618	An insecure deserialization vulnerability exists in Microsoft SQL Server Reporting Services. The vulnerability is due to improper handling of requests to the ReportViewer.aspx page a remote authenticated attacker could exploit this vulnerability by sending a crafted parameter(NavigationCorrector\$ViewState). Successfull exploitation the vulnerability allows the attacker to execute code in the context of the user running the server.
Strike Microsoft SharePoint Workflows XOML Injection	CWE: 91 CVE: 2020-0646	This strike exploits a code injection vulnerability in Microsoft .NET framework. The vulnerability is due to improper sanitization of parameters during Workflow compilation in .NET, which SharePoint relies on to compile and execute workflows. Remote attackers can exploit this flaw by injecting malicious code into Workflow definitions using specially crafted .XOML files, leading to arbitrary code execution on the SharePoint server.
Strike Microsoft Internet Explorer comparator sort method Use-After-Free	CWE: 119 CVE: 2020-0674	This strike exploits a vulnerability in the Microsoft Internet Explorer scripting engine. Specifically, an attacker can craft an HTML page containing a Javascript script which creates an array of objects, and the object is reassigned in a custom sort function which then calls 'CollectGarbage()' resulting in use after free condition due to a dangling pointer. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful exploitation could lead to arbitrary code execution in the security context of the target user.
Strike Microsoft Exchange Server Fixed Cryptographic Key Remote Code Execution	CWE: 502 CVE: 2020-0688	A remote code execution vulnerability exists in Microsoft Exchange Server due to a hardcoded validation key. A remote authenticated attacker may send a crafted serialized 'ViewState' object, which gets deserialized on the server to achieve remote code execution as the 'SYSTEM' user.
Strike SolarWinds Orion API Authentication Bypass	CWE: 287 CWE: 288 CVE: 2020-10148	This strike exploits an authentication bypass vulnerability in SolarWinds Orion API. The vulnerability is due to insufficient validation of path components in a HTTP POST request. A remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the server. A successful attack may result in API commands execution.
Strike Zoho ManageEngine Desktop Central FileStorage getChartImage Command Injection	CWE: 502 CVE: 2020-10189 EXPLOITDB : 48224	This strike exploits a Java deserialization vulnerability in the Zoho ManageEngine Desktop Central. This vulnerability is in the getChartImage function of the FileStorage class, due to lack of proper validation of user-supplied data, which results in deserialization of untrusted data. A remote unauthenticated attacker can exploit this vulnerability by sending crafted HTTP requests to the target server. Successful exploitation results in remote code execution under the context of SYSTEM/root.

Name	References	Description
Strike Sonatype Nexus Repository Manager ContentSelectorsApi Resource Stored Cross-Site Scripting	CWE: 79 CVE: 2020-10203	This strike exploits a stored cross-site scripting vulnerability in Sonatype Nexus Repository Manager. The vulnerability results from inadequate input validation in the content-selectors REST API request within the Java class ContentSelectorsApiResource. This flaw allows an authenticated attacker to inject malicious script code into the database by sending a carefully crafted request to the target server. Successful exploitation of this vulnerability could lead to the execution of arbitrary code within the security context of the user's browser.
Strike rConfig commands.inc.php SQL Injection	CWE: 89 CVE: 2020-10220	This strike exploits a SQL Injection vulnerability in the rConfig server. The vulnerability is caused by insufficient validation of the 'searchField' and 'searchColumn' parameter in the 'commands.inc.php' module. Successful exploitation could allow an attacker to execute SQL command on the target server.
Strike rconfig misconfigured post os command injection	CWE: 78 CVE: 2020-10221	This Strike exploits OS Command Injection Vulnerability against rconfig. The vulnerability is due to Improper Neutralization of elements such as HTTP POST in the configuration. An attacker can exploit this vulnerability by sending OS commands via shell metacharacters in the filename POST parameter. Successful Exploitation would result in the OS command Execution within the context of the user running rconfig.
Strike Advantech WebAccess NMS Save Background Action Directory Traversal	CWE: 22 CVE: 2020-10619	An arbitrary file overwrite vulnerability has been identified in Advantech WebAccess NMS. The vulnerability is caused by the lack of proper input sanitisation on file paths within saveBackground servlet. The vulnerability can be exploited by sending a specially-crafted request, allowing the attacker to delete arbitrary files.
Strike Advantech WebAccess NMS LicenseImportAction Arbitrary File Upload Vulnerability	CVE: 2020-10621	This strike exploits an arbitrary file upload vulnerability in Advantech WebAccess NMS. The vulnerability resides in the insufficient validation of file paths within the licenseImportAction.action endpoint. A remote, unauthenticated attacker could leverage this flaw to upload malicious files, potentially leading to arbitrary code execution under the SYSTEM user context.
Strike Advantech WebAccess NMS download.jsp Directory Traversal Vulnerability	CVE: 2020-10631	This strike exploits a directory traversal vulnerability in Advantech WebAccess NMS. The vulnerability is located in the download.jsp endpoint, where insufficient input validation is performed on the filename parameter. Exploiting this vulnerability allows a remote, unauthenticated attacker to read or delete arbitrary files on the target server, potentially leading to sensitive information disclosure or denial of service.
Strike rConfig search.crud.php OS Command Injection	CVE: 2020-10879 CWE: 74	This strike exploits a OS Command Injection vulnerability in the rConfig server. The vulnerability is in the 'nodeId' parameter in the 'search.crud.php' module, due to failure to properly sanitize the user-supplied input. A remote, authenticated attacker can create a malicious HTTP request resulting in arbitrary command execution on the target system with the privileges of the user running the web server.

Name	References	Description
Strike Tenda AC1900 Router AC15 Model Devicename Remote Code Execution Vulnerability	CVE: 2020-10987 CWE: 78	This strike exploits a remote code execution vulnerability in Tenda AC1900 Router AC15 Model. The vulnerability is due to improper validation of the input parameter deviceName and this value is directly passed to a doSystemCmd function. An unauthenticated attacker could exploit this vulnerability by sending a malicious shellcode through the deviceName parameter and might result in remote code execution.
Strike Microsoft SharePoint DataSet Object Remote Code Execution	CVE: 2020-1147	This strike exploits a remote code execution vulnerability that affects Microsoft .NET Framework, SharePoint, and Visual Studio. This vulnerability is due to improper validation of the source markup of XML file input. An attacker could exploit this vulnerability by enticing a user to open a crafted document or sending maliciously crafted XML content to a server that processes the XML data using the vulnerable library. Successful exploitation allows the attacker to run arbitrary code in the security context of the .NET application.
Strike WordPress Duplicator Plugin Path Traversal	CWE: 22 CVE: 2020-11738	This strike exploits an unauthenticated directory traversal vulnerability in WordPress Duplicator plugin. This vulnerability is due to the implementation of a pair of functions, duplicator_download and duplicator_init. The functions are hooked into init, which are executed when every WordPress page is loaded, whether the user is logged in or not. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the WordPress site. Successful exploitation of this vulnerability could lead to arbitrary file read with the web server privileges.
Strike Apache Airflow Command Injection	CWE: 78 CVE: 2020-11978	This strike exploits remote code/command injection vulnerability in Apache Airflow. This vulnerability was discovered in one of the example DAGs(Directed Acyclic Graph) shipped with Airflow which would allow any user to run arbitrary commands as the user running airflow worker/scheduler(depending on the executor in use). A remote unauthenticated attacker can exploit this vulnerability by sending a crafted request to apache airflow. *NOTE: When running this strike in OneArm mode, first it searches for the example_trigger_target_dag on the target server. If found, then it unpauses the example dag and then creates a DAG(it is a collection of all the tasks that one may want to run), which in this case is creation of a file /tmp/test .
Strike TP-Link NC2XX sysname OS Command Injection	CWE: 78 CVE: 2020-12109	A remote command injection exists in multiple TP-Link Cloud Camera devices (NC2XX) due to lack of user input sanitization. By sending a crafted 'sysname' POST parameter to '/setsysname.cgi' path, a remote authenticated commander may execute arbitrary commands on the target system.
Strike rConfig vendors.crud.php Arbitrary File Upload Vulnerability	CVE: 2020-12255	This strike exploits an arbitrary file upload vulnerability in the rConfig Network Device Configuration Tool. The vulnerability resides in the improper validation of the HTTP multipart/form-data request parameter vendorLogo within the vendors.crud.php script. Exploiting this vulnerability allows a remote authenticated attacker to upload malicious files, potentially leading to arbitrary code execution under the security context of the affected service.

Name	References	Description
Strike rConfig Network Device Configuration Tool devicemgmt.php Cross-Site Scripting	CWE: 79 CVE: 2020-12256	This strike exploits a cross-site scripting vulnerability in rConfig Network Device Configuration Tool. The vulnerability is due to improper validation of the user-supplied request parameter deviceId by devicemgmt.php. A remote attacker could exploit this vulnerability by enticing a victim to open a link or a web page. Successful exploitation could result in the execution of script code in security context of the target users browser.
Strike rConfig Network Device Configuration Tool configDevice.php Cross-Site Scripting	CWE: 79 CVE: 2020-12259	This strike exploits a cross-site scripting vulnerability in rConfig Network Device Configuration Tool. The vulnerability arises from inadequate validation of the 'rid' request parameter in configDevice.php. A remote attacker could exploit this vulnerability by enticing a victim to open a link or a web page. If successfully exploited, this could lead to the execution of script code within the security context of the targeted user's browser.
Strike Roundcube Webmail im_convert_path RCE Vulnerability	CWE: 78 CVE: 2020-12641	This strike exploits remote code execution vulnerability in Roundcube webmail. The vulnerability is due to the im_convert_path configuration setting, which allows a remote, unauthenticated attacker with access to the Roundcube installer to inject system commands. These commands execute whenever a user opens an email containing a "non-standard" image. Successful exploitation could lead to arbitrary command execution.
Strike Centreon RRDdatabase_status_path Command Injection Vulnerability	CVE: 2020-13252	This strike targets a command injection vulnerability in the Centreon Web Application. The issue arises from improper validation of the `RRDdatabase_status_path` parameter in HTTP requests. Exploiting this flaw allows a remote, authenticated attacker to execute arbitrary commands on the server with the privileges of the web server process.
Strike phpGACL acl_admin action parameter Reflected Cross-Site Scripting	CWE: 79 CVE: 2020-13562	This strike exploits a reflected cross-site scripting vulnerability in phpGACL. This vulnerability is due to insufficient validation of action parameter in acl_admin.php. A remote attacker can exploit this vulnerability by enticing a target user into clicking a malicious link. Successful exploitation could result in code-execution, depending on javascript payload embedded in the malicious link. *NOTE: This strike simulates interaction with OpenEMR which uses the vulnerable version of phpGACL, which makes OpenEMR vulnerable. When running this strike in OneArm mode, the credentials used will be admin/pass and requests will be sent to /someuri instead of /openemr/someuri(default) since the OpenEMR docker used is configured that way.
Strike phpGACL acl_admin acl_id parameter Reflected Cross-Site Scripting	CWE: 79 CVE: 2020-13564	This strike exploits a reflected cross-site scripting vulnerability in phpGACL. This vulnerability is due to insufficient validation of acl_id parameter in acl_admin.php. A remote attacker can exploit this vulnerability by enticing a target user into clicking a malicious link. Successful exploitation could result in code-execution, depending on javascript payload embedded in the malicious link. *NOTE: This strike simulates interaction with OpenEMR which uses the vulnerable version of phpGACL, which makes OpenEMR vulnerable. When running this strike in OneArm mode, the credentials used will be admin/pass and requests will be sent to /someuri instead of /openemr/someuri(default) since the OpenEMR docker used is configured that way.

Name	References	Description
Strike Wordpress Plugin BBPress Unauthenticated Privilege Escalation	CWE: 269 CVE: 2020-13693	An authentication bypass vulnerability exists in the bbPress Wordpress plugin. The vulnerability is due to lack of validation on user authorization requests. A remote unauthorized attacker can exploit this vulnerability by sending a crafted HTTP POST request to the system. Successful exploitation results in creating a user with full privileges ('Keymaster' role).
Strike Apache Kylin REST API Command Injection Vulnerability	CVE: 2020-13925	This strike exploits a command injection vulnerability in Apache Kylin. The vulnerability resides in the diag REST API endpoint, specifically in the DiagnosisService class, where user-supplied input is insufficiently validated. An authenticated remote attacker could leverage this flaw by sending crafted HTTP requests, leading to arbitrary command execution on the server.
Strike Apache Unomi OGNL MVEL2 Remote Command Execution	CWE: 20 CVE: 2020-13942	This strike exploits a remote command execution vulnerability found in Apache Unomi. The vulnerability is due to the lack of input validation of Object Graph Navigation Library (OGNL) and MVEL2 for raw user input. The vulnerability can be exploited by an unauthenticated attacker crafting a malicious HTTP POST request. Successful exploitation may result in executing arbitrarily code within the context of the user running the web service.
Strike Apache ActiveMQ Web Console message.jsp Cross-Site Scripting	CWE: 79 CVE: 2020-13947	This strike exploits an cross-site scripting vulnerability in Apache ActiveMQ. The vulnerability is due to insufficient validation of the JMSDestination parameter to message.jsp in the web console. A remote attacker could exploit this vulnerability by enticing a target user to open a malicious crafted link or web page. Successful exploitation could result in code-execution, depending on javascript payload embedded in the malicious link. *NOTE: In OneArm mode, the credentials used for authorization will be admin/admin.
Strike Apache OpenMeetings NetTest Denial of Service	CWE: 835 CVE: 2020-13951	This strike exploits a denial of service vulnerability in Apache OpenMeetings 4.0.0 - 5.0.0. The vulnerability is caused by a lack of rate limiting on NetTest. A remote, unauthenticated attacker can send a large number of requests to the server resulting in network exhaustion and denial of service.
Strike Oracle Business Intelligence Enterprise Edition Path Traversal	CWE: 22 CVE: 2020-14864	This strike exploits a directory traversal vulnerability in Oracle Business Intelligence Enterprise Edition. This vulnerability is due to the getPreviewImage function which is used to get the preview image of a previously uploaded theme logo. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request by manipulating the previewFilePath URL parameter. Successful exploitation of this vulnerability could allow an attacker to read sensitive files, execute arbitrary code, or gain unauthorized access to the system.

Name	References	Description
Strike Oracle WebLogic Server console Authentication Bypass	CWE: 20 CVE: 2020-14882 EXPLOITDB : 48971	This strike exploits an authentication bypass vulnerability in Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). The vulnerability is due to improper configuration of the Path Traversal blacklist of the server URL in the handler class of the WebLogic HTTP access. A remote, unauthenticated attacker can bypass authentication of the administrator console component by sending a simple HTTP GET request to a double-encoded endpoint containing the Console Portal page. Successful exploitation may result in arbitrary command execution in the context of the server process.
Strike Oracle WebLogic Server Remote Code Execution	CWE: 287 CVE: 2020-14883 EXPLOITDB : 48971	This strike exploits an authentication bypass vulnerability in Oracle WebLogic Server. The vulnerability arises from improper validation of user-supplied data sent via HTTP. A remote, unauthenticated attacker can exploit this vulnerability by sending commands through an MVEL expression under the handle of the com.tangosol.coherence.mvel2.sh.ShellSession class. Successful exploitation could allow the attacker to execute arbitrary code on the affected system.
Strike KingComposer plugin for WordPress Cross Site Scripting	CVE: 2020-15299 CWE: 79	This strike exploits a reflected cross-site scripting vulnerability in KingComposer plugin through 2.9.4 for WordPress. The vulnerability takes advantage of kc-online-preset-data parameter to send base64 encoded Javascript. A remote, unauthenticated attacker can exploit this vulnerability by sending a POST request to wp-admin/admin-ajax.php with the action parameter set to kc_install_online_preset. As such, if an attacker used base64-encoding on a malicious payload, and tricked a victim into sending a request containing the payload in the kc-online-preset-data parameter, that malicious payload would be decoded and executed in the victim's browser.
Strike Ivanti MobileIron Remote Code Execution Vulnerability	CWE: 706 CVE: 2020-15505	This strike exploits a remote code execution vulnerability in MobileIron products. The vulnerability exists in a Tomcat Web Service that deserializes user input using the Hessian format. This unsafe deserialization allows malicious input to be executed, leading to potential remote code execution. Attackers can leverage the inconsistency between Apache and Tomcat to bypass access controls and execute malicious payloads by exploiting deserialization vulnerabilities in the Hessian format. Successful exploitation of this vulnerability could allow a remote, unauthenticated attacker to execute arbitrary code on the affected system.
Strike Nagios XI ajaxhelper Command Injection	CWE: 78 CVE: 2020-15901	This strike exploits a command injection vulnerability in the 'ajaxhelper.php' script for Nagios XI. The flaw is due to the insufficient validation of the opts parameter in the 'ajaxhelper.php' script. The flaw may be exploited by an authenticated attacker to execute arbitrary code in the context of the Nagios user on the target server. Note: This strike assumes that the attacker is authenticated and the Cookie and NSP fields are known.
Strike Advantech iView DeviceTreeTable exportTaskMgrRepo rt Directory Traversal	CWE: 22 CVE: 2020-16245	This strike exploits a directory traversal vulnerability in Advantech iView. The vulnerability is due to improper handling of user-supplied path in HTTP requests. A remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the server. A successful attack may result in arbitrary file read, or arbitrary code execution in the security context of SYSTEM.

Name	References	Description
Strike SaltStack Salt API SSH Client Command Injection	CWE: 78 CVE: 2020-16846	This strike exploits a command injection vulnerability in the SSH client for Salt API component of SaltStack Salt. Specifically, when a POST request is made to the rest_cherrypy service the ssh_port parameter is not properly sanitized. The flaw may be exploited by an authenticated attacker to execute arbitrary code in the context of the root user. This flaw can also be exploited by unauthenticated attacker when combining it with CVE-2020-25592. Note: This strike simulates the unauthenticated attacker behaviour.
Strike Microsoft Exchange Server DlpUtils AddTenantDlpPolicy Remote Code Execution	CWE: 94 CVE: 2020-16875	A remote code execution vulnerability exists in Microsoft Exchange Server due to improper validation of cmdlet arguments. A remote authenticated attacker can exploit this vulnerability by running a particular cmdlet with crafted arguments against a vulnerable Exchange server. Successful exploitation could result in the execution of arbitrary commands as SYSTEM.
Strike Fuel CMS Col Parameter SQL Injection Vulnerability	CWE: 89 CVE: 2020-17463	This strike exploits an SQL injection vulnerability in Fuel CMS. This vulnerability lies in the parameter col in permission/items, logs/items, pages/items, navigation/items. An authenticated attacker can exploit this vulnerability by crafting a specially crafted SQL payload. Successful exploitation of this vulnerability could lead to unauthorized access, data leakage and data manipulation.
Strike vBulletin widget_tabbedcontent_tab_panel Remote Code Execution	CVE: 2020-17496	A server-side template injection vulnerability that leads to remote code execution exists in vBulletin due to a logic bug in the patch for CVE-2019-16759. By exploiting it, a remote unauthenticated attacker may execute arbitrary code using server's PHP engine.
Strike Artica Web Proxy apikey Parameter SQL Injection	CWE: 89 CVE: 2020-17506	This strike exploits an SQL injection vulnerability in Artica Web Proxy. This vulnerability is due to improper validation of the apikey parameter of the fw.login.php page. An attacker can send a crafted HTTP request with SQL commands in the vulnerable parameter allowing remote code execution to occur.
Strike Apache Flink FileUploadHandler Arbitrary File Upload	CWE: 22 CVE: 2020-17518	This strike exploits a file upload vulnerability in Apache Flink. The vulnerability is due to insufficient input validation while uploading files in the FileUploadHandler class. A remote, unauthenticated attacker can exploit this vulnerability by submitting a crafted request to the target server results in the writing of an arbitrary file to any location writable by the target server. *NOTE: When running this strike in OneArm mode, a randomly generated file is uploaded in the /tmp directory of the target machine .
Strike Apache Flink JobManager CustomLogHandler Directory Traversal	CWE: 552 CVE: 2020-17519	This strike exploits a directory traversal vulnerability in Apache Flink. The vulnerability is due to insufficient validation of user supplied file path in JobManagerCustomLogHandler class. An unauthenticated remote attacker can exploit the vulnerability by sending a specially-crafted request to the target server. Successful exploitation results in potentially sensitive file-data being returned in the response from server. *NOTE: When running this strike in OneArm mode, the strike attempts to read data from a potentially sensitive file (/etc/passwd or /etc/fstab).

Name	References	Description
Strike Apache Struts ONGL Remote Code Execution	CWE: 94 CVE: 2020-17530	A remote command execution vulnerability exists in Apache Struts framework as a result of no sanitization of user supplied data. By sending a crafted request, a remote attacker may execute arbitrary OS commands with the server privilege.
Strike Apache Kylin-migrate API OS Command Injection	CWE: 78 CVE: 2020-1956	A command injection vulnerability exists in in Apache Kylin project versions 2.3.0-2.3.2, 2.4.0-2.4.1, 2.5.0-2.5.2, 2.6.0-2.6.4 and 3.0.0. The vulnerability is due to lack of validation for user-supplied input to 'migrate' REST API endpoint. A remote authenticated attacker may execute arbitrary commands by sending a crafted POST request.
Strike Palo Alto Networks Management Interface Command Injection	CVE: 2020-2038 CWE: 78	This strike exploits a management interface command injection vulnerability in Palo Alto Networks PAN-OS. This vulnerability is due to insufficient filtering of the user input in the execute method of the RestApi Class. A remote authenticated attacker can exploit this vulnerability to execute arbitrary OS commands with root privileges. Note: In one_arm this strike simulates the attack using a fixed API key.
Strike PHP-Fusion Downloads php Command Injection	CWE: 269 CVE: 2020-24949	This strike simulates a command injection vulnerability in PHP-Fusion. The vulnerability is due to insufficient validation of HTTP request parameters in downloads.php. A remote unauthenticated attacker could exploit this vulnerability by sending an crafted HTTP request to the vulnerable server. Successful exploitation of this vulnerability could allow the attacker to execute command in the security context of the running server.
Strike Advantech R-SeeNet device_position.php SQL Injection Vulnerability	CVE: 2020-25157	This strike exploits a SQL injection vulnerability in Advantech R-SeeNet. The vulnerability exists due to insufficient validation of the device_id parameter in the device_position.php file. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted HTTP requests, potentially leading to the retrieval of sensitive information from the database.
Strike WordPress File Manager connector_minimal.php Improper Access Control	CWE: 434 CVE: 2020-25213	This strike exploits an improper access control vulnerability in the File Manager plugin for WordPress. The vulnerability arises from inadequate access control for the connector_minimal.php file during file uploads. This allows an unauthenticated attacker to upload arbitrary files, including potentially malicious PHP files, posing a risk of executing arbitrary code. A remote, unauthenticated attacker could exploit this vulnerability by submitting a carefully crafted request to a WordPress server with the File Manager Plugin installed. Successful exploitation could lead to the unauthorized upload of arbitrary files, potentially resulting in the execution of arbitrary code within the security context of the WordPress server.
Strike D-Link DNS-320 system_mgr.cgi Command Injection	CVE: 2020-25506 CWE: 78	This strike exploits a Command Injection vulnerability in D-Link DNS-320 FW. The vulnerability is due to the f_ntp_server parameter, which is not Sanitized successfully before being used. A remote, unauthenticated attacker could exploit this vulnerability by injecting the commands into the f_ntp_server parameter, which leads to arbitrary command execution. Successful exploitation could allow the attacker to execute arbitrary code on the affected device.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike D-Link DSR-250N Denial of Service	CWE: 284 CVE: 2020-26567	This strike exploits a vulnerability inside D-Link Wireless N Unified Service Routers (DSR-250N) 3.12 that can cause a denial of service attack. The device which allows unauthenticated attackers in the same local network to execute a CGI script which reboots the device. The attack can be triggered without authentication.
Strike Ruckus IoT Controller Web UI OS Command Injection	CWE: 862 CVE: 2020-26878	An OS command injection vulnerability exists in Ruckus IoT Controller 1.5.1.0.21 and prior due to lack of user input validation. The vulnerability exists in the '/service/v1/createUser' endpoint which is in charge of new users creation. By sending a crafted HTTP POST data, a remote authenticated attacker may execute arbitrary OS commands as the root user.
Strike Ruckus IoT Controller Web UI Authentication Bypass	CWE: 798 CVE: 2020-26879	An authentication bypass vulnerability exists in Ruckus IoT Controller 1.5.1.0.21 and prior. The vulnerability exists due to a hardcoded token used when the 'Authorization' HTTP header has a specific value. By sending a crafted HTTP request, a remote attacker may obtain unauthorized access to the device.
Strike Netgear JGS516PE Devices Missing Function Level Access Control Vulnerability	CVE: 2020-26919 CWE: 306	This strike exploits an improper access control at the function level vulnerability on NETGEAR JGS516PE devices. The vulnerability arises because the publicly accessible "login.html" page lacks restrictions on executing debug actions. A remote unauthenticated attacker can exploit this by sending arbitrary code in debugCmd through post request. Successful exploitation could allow users execute system commands.
Strike Cisco Security Manager AuthTokenServlet Insecure Deserialization	CWE: 502 CVE: 2020-27131	The strike exploits an insecure deserialization vulnerability in Cisco Security Manager. The vulnerability is due to insufficient validation of serialized data, passed via HTTP(S) request to /CSConm/servlet/com.cisco.nm.cmf.servlet.AuthTokenServlet, causing deserialization of untrusted data while having exploitable libraries in the code path. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted serialized object to the target server. Successful exploitation can result in arbitrary code execution as root.
Strike Arcserve D2D getNews External Entity Injection	CWE: 611 CVE: 2020-27858	This strike exploits an XXE or XML External Entity injection vulnerability in Arcserve D2D. The vulnerability arises from inadequate validation of XML data within the getNews method. An unauthenticated remote attacker could exploit this vulnerability by transmitting malicious XML data in HTTP requests to the target server. Successful exploitation may lead to the disclosure of information within the context of SYSTEM.
Strike SolarWinds Network Configuration Manager VulnerabilitySettings Arbitrary File Write	CWE: 22 CVE: 2020-27871	This strike exploits an arbitrary file write vulnerability that has been reported in SolarWinds Network Configuration Manager. The vulnerability is due to insufficient validation of file types for vulnerability announcement data files in VulnerabilitySettings.aspx, combined with a lack of restriction on destination paths. A remote, authenticated attacker can exploit this vulnerability by submitting a crafted request to the target server. Successful exploitation results in the writing of an arbitrary file to a location chosen by the attacker, potentially leading to execution of arbitrary code as SYSTEM.

Name	References	Description
Strike Nagios XI do_update_user Stored Cross-site Scripting	CWE: 79 CVE: 2020-27988	A stored cross-site scripting vulnerability exists in Nagios XI versions prior to 5.7.5. The vulnerability is due to insufficient sanitization of username in 'users.php'. A remote authenticated attacker can exploit this vulnerability by sending crafted HTTP request to the server. Successful exploitation could result in arbitrary JavaScript execution on the victim's browser.
Strike Oracle E-Business Suite Advanced Outbound Telephony CVE-2020-2854 Cross-Site Scripting	CWE: 79 CVE: 2020-2854	A cross-site scripting vulnerability has been reported in the Advanced Outbound Telephony component of Oracle E-Business Suite. A remote attacker can exploit this vulnerability by enticing a target user into opening a crafted link. Successful exploitation could result in the execution of script code in security context of the target users browser.
Strike Oracle E-Business Suite Advanced Outbound Telephony Cross-Site Scripting	CWE: 79 CVE: 2020-2871	This strike exploits a cross-site scripting vulnerability in the User Interface of the Advanced Outbound Telephony component in Oracle E-Business Suite. A remote attacker can exploit this vulnerability by enticing a target user into clicking on a crafted link. Successful exploitation could result in the execution of script code in security context of the target users browser.
Strike D-Link DIR-825 Check Browser Buffer Overflow	CWE: 119 CVE: 2020-29557	This strike exploits a Buffer Overflow vulnerability in the web component of D-Link DIR-825. The vulnerability is due to improper handling of GET parameters processed by the mg_get_var function. The function retrieves the data using a fixed buffer size of 512 bytes, but the actual allocated buffer for storing the parameters is only 128 bytes. When the attacker sends a request with data larger than the buffer, it causes an overflow. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request larger than the buffer limit to the target server. Successful exploitation could result in memory corruption.
Strike Zyxel Products Use of Hard-Coded Credentials	CWE: 522 CVE: 2020-29583	This strike exploits an use of Hard-Coded Credentials Vulnerability in Zyxel Multiple Products. This vulnerability is due to an undocumented account (zyfwp) with an unchangeable password. The account is designed to deliver automatic firmware updates to connected access points through FTP. A remote, unauthenticated attacker could exploit this vulnerability to gain unauthorized access to the affected device, potentially leading to further compromise of the network.
Strike Cisco IP Phones Web Server sprintf Denial of Service Vulnerability	CWE: 20 CVE: 2020-3161	This strike exploits a stack-based buffer overflow vulnerability in Cisco IP Phones. The vulnerability is due to a lack of proper input validation in HTTP requests. The libHTTPService.so library processes parameters from the /deviceconfig/setActivationCode endpoint using sprintf without checking their length, allowing an attacker to overflow the stack-based buffer. This can cause a device crash or enable remote code execution. A remote, unauthenticated attacker could exploit this by sending a crafted HTTP request to the web server of a targeted device. A successful exploitation could allow an attacker to reload an affected IP phone, causing denial of service, or ultimately result in remote code execution with root privileges.

Name	References	Description
Strike Cisco UCS Director ApplianceStorageUtil Directory Traversal	CWE: 22 CVE: 2020-3239	A directory traversal vulnerability exists in Cisco UCS Director. The vulnerability is due to insufficient validation of user input within 'ApplianceStorageUtil' class. A remote authenticated attacker can exploit the vulnerability by sending malicious requests to the target server. Successful exploitation could result in the arbitrary file write and remote code execution under the security context of web server.
Strike Cisco UCS Director Directory Traversal Vulnerability	CVE: 2020-3251	This strike exploits a directory traversal vulnerability in Cisco UCS Director. The vulnerability exists due to insufficient validation of user input within the MyCallable class when processing file upload requests. A remote authenticated attacker could leverage this flaw to write arbitrary files to the server, potentially leading to remote code execution under the web server's security context.
Strike Cisco ASA and FTD Web Services Path Traversal	CVE: 2020-3452 CWE: 22	This strike exploits a Path Traversal vulnerability in web services interface of Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD). The vulnerability is due to improper input validation of URLs in HTTP requests processed by the device. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. Successful exploitation allows the attacker to view arbitrary files within the web services file system on the targeted device.
Strike Nagios XI Manage Plugins Command Injection	CWE: 78 CVE: 2020-35578	This strike exploits a command injection vulnerability in the admin webpage 'monitoringplugins.php' script for Nagios XI. The flaw is due to the insufficient validation of the 'uploadedfile' multipart filename. The flaw may be exploited by an authenticated attacker to execute arbitrary code in the context of the Nagios user on the target server.
Strike Webmin Package Updates update.cgi Command Injection	CWE: 78 CVE: 2020-35606	This strike exploits a command injection vulnerability in Webmin. The vulnerability is due to the insufficient validation of input in the Package Updates module. A remote attacker could exploit this vulnerability by sending a crafted request to the target system. Successful exploitation of this vulnerability could result in arbitrary command execution on the target system.
Strike Twitter TwitterServer HistogramQueryHandler Cross-Site Scripting	CWE: 79 CVE: 2020-35774	This strike exploits a reflected XSS vulnerability in twitter-server. This vulnerability is due to insufficient validation on user supplied input in the /admin/histograms API method. A remote unauthenticated attacker can exploit this vulnerability by enticing a target user into clicking a malicious link. Successful exploitation could result in code-execution in the context of the browser.
Strike Cisco Adaptive Security Appliance and Firepower Threat Defense Cross-Site Scripting	CVE: 2020-3580 CWE: 79	This strike exploits a cross-site scripting (XSS) vulnerability in Cisco Adaptive Security Appliance and Cisco Firepower Threat Defense. The vulnerability is due to improper input validation of web content within the WebVPN functionality of these devices. An unauthenticated, remote attacker could exploit this flaw to launch XSS attacks against users of the web services interface. If successfully exploited, the vulnerability could result in session hijacking or theft of sensitive information.

Name	References	Description
Strike OpenEMR Backup php Command Injection	CWE: 78 CVE: 2020-36243	This strike exploits a command injection vulnerability in OpenEMR. This vulnerability is due to insufficient sanitization for the user-supplied data in the backup.php. A remote authenticated attacker can exploit this vulnerability by sending crafted requests to the target server. Successful exploitation could result in arbitrary command execution in the security context as web server. *NOTE: When running this strike in OneArm mode, the requests will not be sent to /openemr/someuri , instead will be sent to /someuri , since the openemr server docker used, is configured that way.
Strike VMware Cloud Director Expression Language Authenticated Java template injection	CWE: 74 CVE: 2020-3956	A command injection vulnerability exists in VMware Cloud Director. The vulnerability is due to the lack of sanitization while parsing input passed to 'hostname' parameter within the Smtp configuration form. An authenticated attacker can exploit this vulnerability by crafting a malicious HTTP PUT request. Successful exploitation results in full control of the cloud director platform.
Strike VMware Multiple Products ApplianceSslCertificateService Command Injection	CWE: 77 CVE: 2020-4006	This strike exploits a command injection vulnerability in VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector. The vulnerability is due to improper validation of user input in the 'san' parameter. The flaw may be exploited by an authenticated attacker to execute arbitrary code in the context of the service running on the target server.
Strike IBM Spectrum Protect Plus hostname Command Injection	CVE: 2020-4211 CWE: 74	This strike exploits a command injection vulnerability in IBM Spectrum Protect Plus. The vulnerability is due to a combination of missing authentication of the hostname uri and a lack of input sanitization for injection or invalid characters in the hostname parameter. When an attacker sends an HTTP POST request to "/emi/api/hostname", command execution can occur.
Strike IBM Spectrum Protect Plus uploadHttpsCertificate Command Injection	CVE: 2020-4241 CWE: 78	This strike exploits a command injection vulnerability in IBM Spectrum Protect Plus. The vulnerability is due to a lack of input sanitization for injection or invalid characters in the filename parameter. When an attacker sends an HTTP POST request to the "/emi/api/uploadhttpscertificate" URI, command execution can occur.
Strike Gila CMS Image Upload Remote Code Execution	CWE: 434 CVE: 2020-5514	This strike exploits a remote code execution vulnerability in Gila CMS. The vulnerability is due to improper validation of user supplied files during image upload. An attacker can cause a file write to the tmp folder that is not an image by requesting a thumbnail of a remote non-image file and subsequently requesting the written file, enabling the creation and execution of arbitrary PHP script files. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the targeted server. Successful exploitation of the vulnerability could lead to arbitrary code execution under the security context of the service.

Name	References	Description
Strike Plex Media Server unpickle Dict Insecure Deserialization	CVE: 2020-5741 CWE: 502	This strike exploits an insecure deserialization vulnerability in Plex Media Server. The vulnerability is due to the unsafe deserialization of Dict files, which are unpickled without validation when loaded for a given plugin. An authenticated attacker can remotely deliver a malicious Dict file via the camera upload feature. By setting the Windows-only Plex variable LocalAppDataPath to the newly created photo library, the deserialization process is triggered, potentially leading to remote code execution.
Strike Nagios XI mibs Command Injection	CWE: 78 CVE: 2020-5791	This strike exploits a command injection vulnerability in the 'mibs.php' script for Nagios XI. The flaw is due to the insufficient validation of the file parameter in the 'mibs.php' script. The flaw may be exploited by an authenticated attacker to execute arbitrary code in the context of the Nagios user on the target server. Note: This strike assumes that the attacker is authenticated and the Cookie and NSP fields are known.
Strike Multiple F5 BIG-IP products Directory Traversal	CWE: 94 CVE: 2020-5902 EXPLOITDB : 48642 EXPLOITDB : 48643	This strike exploits a directory traversal vulnerability in multiple F5 BIG-IP products. The vulnerability is due to improper handling of user-supplied path in HTTP requests. A remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the server. A successful attack may result in arbitrary file read, write or remote code execution in the security context of ROOT.
Strike Google Chrome AudioArray Allocate Data Race	CWE: 119 CVE: 2020-6388 GOOGLE: 1999	This strike exploits a vulnerability in Google Chrome. Specifically, an out of bounds memory access occurs when the AudioArray::Allocate function is invoked in a specific manner. When this happens a denial of service condition, or potentially remote code execution, may occur.
Strike Google Chrome USB OnServiceConnectionError Use After Free	CWE: 416 CVE: 2020-6541 GOOGLE: 2068	This strike exploits a vulnerability in Google Chrome. Specifically, javascript can be crafted in such a way that the 'OnServiceConnectionError' function calls 'Resolve' which invokes a user-defined function. If this user function calls USB::getDevices an invalid loop iterator is set. When this loop cycles, a use after free condition can occur. When this happens a denial of service, or potentially remote code execution, may be possible.
Strike Google Chrome MediaElementEvent Listener UpdateSources Use-After-Free	CWE: 416 CVE: 2020-6549 GOOGLE: 2063	This strike exploits a vulnerability in Google Chrome. Specifically, a Use-After-Free condition occurs when the MediaElementEventListener::UpdateSources function is invoked in a specific manner. When this happens a denial of service condition, or potentially remote code execution, may occur.

Name	References	Description
Strike Eaton Intelligent Power Manager system_srv Command Injection	CWE: 78 CVE: 2020-6651	A command injection vulnerability exists in Eaton Intelligent Power Manager 1.67 and prior, due to lack of user input sanitization. An authenticated remote attacker may execute arbitrary OS commands as a superuser by providing a crafted filename parameter when uploading a configuration file.
Strike dotCMS CMSFilter assets Access Control Weakness	CWE: 22 CVE: 2020-6754	An access control weakness has been reported in the dotCMS content management system. The vulnerability is due to insufficient path validation in the CMSFilter class, if the dotCMS installation stores its assets under the tomcats webapps/ROOT/assets directory. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted HTTP request to the targeted server. Successful exploitation of this vulnerability could allow the attacker to access restricted resources or execute arbitrary code in the security context of the target service.
Strike Mozilla Firefox ReadableStreamCloseInternal Out of Bounds Access	CWE: 125 CVE: 2020-6806 GOOGLE: 2005	This strike exploits a vulnerability in Spidermonkey, the Javascript engine of Mozilla Firefox. An attacker can craft Javascript promise resolutions in such a way that make it possible to cause an out-of-bounds read off the end of an array resized during script execution. This can lead to a denial of service or potentially allow for remote code execution to occur.
Strike Liferay Portal JSON Web Service Insecure Deserialization Vulnerability	CVE: 2020-7961 CWE: 502 EXPLOITDB : 48332	This strike exploits an insecure deserialization vulnerability in Liferay Portal. The vulnerability is due to improper sanitization of user supplied input. Exploiting this vulnerability could allow remote, unauthenticated attackers to execute arbitrary code on the target server in the context of the user running the server.
Strike Intellian Aptus Web libagent.cgi OS Command Injection	CWE: 78 CVE: 2020-7980	A remote command injection vulnerability exists in Intellian Aptus Web due to lack of user authentication when handling HTTP CGI requests. By sending a crafted JSON file with a POST request, a remote unauthenticated attacker may execute arbitrary system commands as the system's superuser.
Strike Ruby on Rails locals render Remote Code Execution	CWE: 94 CVE: 2020-8163	A remote code execution vulnerability exists in Ruby on Rails versions 5 < 5.0.1 and 4 < 4.2.11.2, due to lack of user input validation. The vulnerability manifests itself whenever the 'locals' value for a 'render' call is set to 'params' value. Remote attackers may exploit applications containing the up-mentioned pattern by sending a crafted HTTP request to obtain arbitrary code execution.
Strike Citrix Application Delivery Controller Authorization Bypass via pcidss.php report Function	CWE: 284 CVE: 2020-8193	An authorization bypass vulnerability exists in Citrix Application Delivery Controller (ADC) and Gateway. This vulnerability can be triggered by calling the function report() in the PHP pcidss.php script. The flaw may be exploited by an unauthenticated attacker to access certain protected URL endpoints.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Citrix Application Delivery Controller Information Disclosure via file_download Function	CWE: 20 CVE: 2020-8195	An information disclosure vulnerability exists in Citrix Application Delivery Controller (ADC) and Gateway. This vulnerability can be triggered by calling the function file_download() in the PHP rapi.php script. The flaw may be exploited by an authenticated attacker to access sensitive data. This flaw can also be exploited by unauthenticated attacker when combining it with CVE-2020-8193.
Strike Squid Reverse Proxy Host Header Buffer Overflow	CWE: 119 CVE: 2020-8450	A stack-based buffer overflow vulnerability exists in Squid before 4.10 due to incorrect buffer management, when acting as a reverse proxy. By sending a crafted HTTP request with a host string longer than 255 characters in the 'Host' header, a remote attacker may achieve remote code execution on the target host.
Strike Trend Micro InterScan Web Security Virtual Appliance Password Command Injection	CWE: 78 CVE: 2020-8466	This strike exploits a command injection vulnerability in Trend Micro InterScan Web Security Virtual Appliance. The vulnerability is due to improper validation of user-supplied data in HTTP requests. The vulnerability is due to failure to validate the parameter 'passwd' for command injection characters. A remote, unauthenticated attacker can exploit the vulnerabilities by sending a malicious request to the target server. Successful exploitation of these vulnerabilities could allow arbitrary command execution on the target server in the security context of iscan account.
Strike Trend Micro Apex One and OfficeScan Directory Traversal	CWE: 23 CVE: 2020-8470	This strike exploits a directory traversal vulnerability in Trend Micro Apex One and OfficeScan. The vulnerability is due to a lack of proper validation of user-supplied filename in BinaryDataBlock parameter when handling requests to cgiLog.exe for CMDHL_SET_SPYWARELOG and CMDHL_SET_SPYWARE_BACKUP_MANIFEST commands. An attacker, without authentication, could potentially exploit this vulnerability by sending a carefully crafted request to the target server. Successful exploitation in the worst case could lead to deletion of arbitrary file under the security context of SYSTEM.
Strike DrayTek Vigor keyPath OS Command Injection	CWE: 74 CVE: 2020-8515	An unauthenticated remote command injection vulnerability exists in DrayTek Vigor2960 1.3.1_Beta, Vigor3900 1.4.4_Beta, Vigor300B 1.3.3_Beta, 1.4.2.1_Beta and 1.4.4_Beta routers, due to lack of user input sanitization. By sending a crafted 'keyPath' HTTP parameter, a remote unauthenticated attacker may execute commands as the system's superuser.
Strike Horde Webmail data.php Code Injection Remote Code Execution	CWE: 94 CVE: 2020-8518 EXPLOITDB : 48215	A PHP code injection vulnerability exists in Horde Groupware Webmail Edition 5.2.22 due to lack of user-supplied data sanitization. Remote authenticated attackers may send a crafted 'quote' parameter in a HTTP request to 'mnemo/data.php' to achieve PHP code execution.

Name	References	Description
Strike Trend Micro Apex One and OfficeScan Directory Traversal CVE 2020-8599	CWE: 434 CVE: 2020-8599	This strike exploits a directory traversal vulnerability in Trend Micro Apex One and OfficeScan. The vulnerability is due to improper validation of user-supplied file name in the X_DTAS_Archive_Filename HTTP header when handling a request for sample file upload. Since a remote unauthenticated attacker can control both the file name and file content, this directory traversal vulnerability could allow the attacker to modify executable files in the target system, which could then lead to remote code execution in the context of IUSR account.
Strike PlaySMS Server-Side Template Injection	CVE: 2020-8644 CWE: 94	This strike exploits a Server Side Template Injection vulnerability in PlaySMS. The vulnerability is due to improper sanitization of user supplied input. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request. Successful exploitation allows the attacker to execute remote code under the context of the running process.
Strike EyesOfNetwork autodiscovery Privilege Escalation	CWE: 269 CVE: 2020-8655	This strike exploits a privilege escalation vulnerability in the web component of EyesOfNetwork. The vulnerability arises from improper sudoers configuration, which allows the apache user to run arbitrary commands as root via a crafted NSE (Nmap Scripting Engine) script for nmap. A remote authenticated attacker can exploit this vulnerability by crafting a specific NSE script for nmap. Successful exploitation of this vulnerability can lead to complete control over the affected system. This vulnerability is chained with CVE-2020-8656, which enables the creation of new user credentials. In this CVE these credentials are used to log in and exploit the privilege escalation flaw.
Strike Pi-hole Web DHCP Static Lease Remote Code Execution	CWE: 78 CVE: 2020-8816	This strike exploits a command injection vulnerability in the web component of Pi-hole. The vulnerability is due to improper input validation. A remote, authenticated attacker could exploit this vulnerability by configuring a DHCP static lease to hold malicious command in the MAC address field. Successful exploitation could result in arbitrary command execution under the security context of the root user.
Strike Webmin log_parser.pl Stored Cross-Site Scripting	CWE: 74 CVE: 2020-8821	A stored XSS vulnerability exists in Webmin 1.941 and earlier, affecting the Command-Shell module. The flaw is due to lack of HTML character escaping when rendering log entries and is located in 'shell/log_parser.pl' script. An authenticated remote attacker may send a crafted POST body to obtain arbitrary JavaScript execution on a target user's browser.
Strike ZyXEL NAS weblogin.cgi OS Command Injection	CWE: 78 CVE: 2020-9054	An OS command injection vulnerability exists in multiple ZyXEL products due to insufficient user input sanitization when parsing the 'username' parameter. By sending a crafted HTTP request, a remote unauthenticated attacker may execute arbitrary OS commands as a superuser.

Name	References	Description
Strike TP-Link TL-WR849N cgi OS Command Injection	EXPLOITDB : 48155 CWE: 78 CVE: 2020-9374	An OS command injection flaw exists in TP-Link TL-WR849N due to lack of user input sanitization. The vulnerability resides in router's 'Diagnostics' area, where tests such as 'ping' and 'traceroute' may be performed. By sending a crafted HTTP POST request, a remote unauthenticated attacker may execute arbitrary commands on the target system.
Strike Centreon server_ip field OS Command Injection	CWE: 78 CVE: 2020-9463	This strike exploits a command injection vulnerability in Centreon 19.10. The vulnerability is due to improper validation of the server_ip parameter in a HTTP request. An authenticated attacker could exploit this by sending a maliciously crafted request to the server. A successful attack may result in arbitrary command execution in the context of the server process.
Strike Apache Tomcat PersistenceManager Insecure Deserialization	CWE: 502 CVE: 2020-9484	An insecure deserialization vulnerability exists in Apache Tomcat. The vulnerability is due to insufficient validation of a cached session file before deserialization. An attacker can exploit this vulnerability by crafting a malicious HTTP request. Successful exploitation results in full control of the target server.
Strike Apache httpd HTTP2 Cache-Digest Header Parsing Memory Corruption	CWE: 444 CVE: 2020-9490	This strike exploits a memory corruption vulnerability in the mod_http2 module of the Apache HTTP server. The vulnerability is due to improper handling of Cache-Digest headers. During base64 decoding of the Cache-Digest header, the function h2_push_diary_digest_set() interprets the first 2 bytes as log2 results. The subsequent calculation of a signed integer N based on these log2 values can result in a negative value, leading to an integer underflow which triggers memory corruption. An attacker could exploit this flaw by sending a specially crafted Cache-Digest header, manipulating variables and triggering an integer underflow, potentially leading to remote code execution on the affected server.
Strike Apache OFBiz XMLRPC Insecure Deserialization	CVE: 2020-9496 CWE: 502	This strike exploits an insecure deserialization vulnerability in Apache OFBiz. The vulnerability is a result of insufficient validation of XML-RPC requests in the SerializableParser class. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to a vulnerable server. Successful exploitation can lead to remote code execution, in the context of the user running the server.
Strike Apple Safari WebKit Incorrect ArithNegate Leads to Out Of Bounds Access	CVE: 2020-9802 GOOGLE: 2020	This strike exploits a vulnerability in Apple Webkit. Specifically, an attacker can craft JavaScript in such a way that Checked and Unchecked ArithNegate operations are incorrectly swapped during Common Subexpression Elimination. This will lead to out-of-bounds memory access on an array after being JIT compiled.
Strike Cisco HyperFlex HX storfs-asup Handling Remote Command Execution	CWE: 78 CVE: 2021-1498	This strike exploits a remote command execution vulnerability in Cisco HyperFlex. The vulnerability is due to improper sanitization of user supplied data. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could lead to execution of arbitrary code in the context of target process.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike SonicWall SMA 100 Appliances Stack-Based Buffer Overflow	CWE: 787 CVE: 2021-20038	This strike exploits stack-based buffer overflow vulnerability in SonicWall SMA 100 Appliances. This vulnerability arises from how environment variables are concatenated into a string within mod_cgi.so and also that the attacker-provided QUERY_STRING is not subjected to any type of length check. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted request to the target server. Successfully exploiting this vulnerability could allow attacker to potentially execute code as a 'nobody' user or crash the affected system.
Strike ManageEngine OpManager Remote Directory Deletion	CWE: 22 CVE: 2021-20078	This strike exploits a directory traversal vulnerability in Zoho ManageEngine OpManager builds below 125346. The vulnerability is due to improper handling of user-supplied path in HTTP requests. A remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the server. A successful attack may result in arbitrary file deletion, which could result in a denial of service.
Strike Zoho ManageEngine ServiceDesk Plus Custom Schedules Command Injection Vulnerability	CVE: 2021-20081	This strike exploits an arbitrary command execution vulnerability in Zoho ManageEngine ServiceDesk Plus. The vulnerability resides in the improper validation of user input within the custom-schedules module. A remote, authenticated attacker could leverage this flaw by sending specially crafted requests, leading to arbitrary command execution and potential remote code execution under the SYSTEM security context.
Strike Arcadyan Buffalo Firmware Path Traversal	CWE: 22 CVE: 2021-20090	This strike exploits a directory traversal vulnerability in Arcadyan Buffalo Firmware. This vulnerability is due to the improper access permission set for a list of folders and files. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation of this vulnerability could lead to read sensitive files, such as configuration files, credentials, or other sensitive information.
Strike Draytek VigorConnect DownloadFileServlet Path Traversal Vulnerability	CWE: 22 CVE: 2021-20123	This strike exploits a local file inclusion vulnerability in Draytek VigorConnect. The vulnerability exists in the file download functionality of the DownloadFileServlet endpoint. A remote, unauthenticated attacker could leverage this vulnerability to download arbitrary files from the vulnerable server with root privileges.
Strike Zoho ManageEngine ADManager Plus Unrestricted File Upload Vulnerability cve_2021_20130	CVE: 2021-20130	This strike exploits an unrestricted file upload vulnerability in Zoho ManageEngine ADManager Plus. The vulnerability exists due to insufficient validation of uploaded files in the PasswordExpiryAction class. A remote authenticated attacker can leverage this flaw to upload malicious files, potentially leading to remote code execution with SYSTEM privileges.
Strike Adobe Magento DownloadCss.php Cross-site Scripting	CWE: 79 CVE: 2021-21029	A reflected cross-site scripting vulnerability exists in Adobe Magento. The vulnerability is due to insufficient sanitization of a file resource identifier in 'DownloadCss.php'. A remote authenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the server. Successful exploitation could result in arbitrary JavaScript execution in victim's browser.

Name	References	Description
Strike Oracle WebLogic Server JNDI Injection	CWE: 610 CVE: 2021-2109	This strike exploits a JNDI injection vulnerability in Oracle Weblogic Server. This vulnerability is due to improper handling user supplied data. A remote, authenticated attacker can exploit this vulnerability by sending a crafted request to a vulnerable server. Successful exploitation results in the target server retrieving a potentially malicious serialized object from an attacker controlled server which may lead to the execution of arbitrary code under the security context of the affected server. *NOTE: When running this strike in OneArm mode, the oracle weblogic server will attempt to make a ldap request to a ldap listener(JNDI server) running on localhost to retrieve the serialized object.
Strike Oracle E-Business Suite Common Applications Calendar Cross-Site Scripting	CWE: 79 CVE: 2021-2114	This strike exploits a reflected cross-site scripting vulnerability in the Common Applications Calendar component in Oracle E-Business Suite. The vulnerability is due to the use of untrusted user input from requests when constructing HTML output. A remote attacker can exploit this vulnerability by enticing a target user into clicking a malicious link. Successful exploitation could result in code-execution, depending on javascript payload embeeded in the malicious link.
Strike OneDev Platform AttachmentUploadServlet Insecure Deserialization	CWE: 502 CVE: 2021-21242	This strike exploits an insecure deserialization vulnerability in OneDev Platform. The vulnerability is due to insufficient validation of request processed in AttachmentUploadServlet servlet. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted request. Successful exploitation would result in arbitrary code execution without authentication.
Strike OneDev Platform KubernetesResource Insecure Deserialization	CWE: 502 CVE: 2021-21243	This strike exploits an Insecure Deserialization vulnerability in the OneDev Platform. The vulnerability occurs due to an API which exposes two methods that deserialize untrusted data from the request body. These API methods do not enforce any authentication checks so it could allow an unauthenticated attacker to execute arbitrary code on the target system. *NOTE: When running this strike in OneArm mode, the strike sends a DNS request to example.com or creates a new file with some data in the "C://" directory depending on the variant.
Strike OneDev Platform PreAuth Access Token Leak	CWE: 862 CVE: 2021-21246	This strike exploits a lack of authentication vulnerability in OneDev Platform. Attackers can send crafted request to the endpoint /users/{id} where there are no security checks enforced, so it is possible to retrieve arbitrary user details including their Access Tokens. *NOTE: When running this strike in OneArm mode, the strike attempts to read information containing access token for the user with id equals 1.
Strike Git Source Code Management Out-of-Order Checkout Improper Link Resolution	CWE: 59 CVE: 2021-21300	This strike exploits an improper link resolution in the checkout mechanism of Git Source Code Management. An out-of-order checkout triggered by a delayed checkout or checkout-index may result in an improper validation of a file system resource type prior to performing a file write operation. A remote attacker can exploit this vulnerability by enticing a user to clone a malicious repository. Successful exploitation can result in remote code execution in the context of the git process.

Name	References	Description
Strike VMware vCenter vSphere Client Arbitrary File Upload	CWE: 269 CVE: 2021-21972 EXPLOITDB : 49602	This strike exploits a file upload vulnerability in vSphere Client component of VMware vCenter. An remote unauthenticated attacker can send a malicious HTTP POST request to upload an arbitrary file via '/ui/vropspluginui/rest/services/uploadova' api. Successful exploitation may lead to creation and execution of arbitrary files with the context of the NT AUTHORITY\SYSTEM for windows and vsphere-ui user for linux.
Strike VMware View Planner Arbitrary File Upload	CWE: 434 CVE: 2021-21978 EXPLOITDB : 49602	This strike exploits a file upload vulnerability in VMware View Planner. An remote unauthenticated attacker can send a malicious HTTP POST request to upload an arbitrary file via 'logupload' endpoint. Successful exploitation can lead to execution of arbitrary code on the target system with root privileges.
Strike VMware vCenter Server Virtual SAN Code Execution	CWE: 20 CVE: 2021-21985	The vSphere Client (HTML5) contains a remote code execution vulnerability due to lack of input validation in the Virtual SAN Health Check plug-in which is enabled by default in vCenter Server. The flaw may be exploited by an unauthenticated attacker to execute arbitrary code in the context of the service running on the target server.
Strike VMware vCenter Server AsyncTelemetryController Arbitrary File Write	CWE: 434 CVE: 2021-22005	An arbitrary file upload vulnerability exists in VMware vCenter Server. The vulnerability is due to insufficient validation of collector IDs and collector instance IDs in requests handled by the AsyncTelemetryController class. A remote attacker could exploit this vulnerability by sending crafted requests to the target server resulting in execution of arbitrary code by the server.
Strike ExifTool DjVu Remote Code Execution	CWE: 74 CVE: 2021-22204	This strike exploits an improper neutralization of directives in dynamically evaluated code ('eval injection') in ExifTool. An remote unauthenticated attacker can supply a malicious crafted DjVu file to be processed via ExifTool. Successful exploitation may lead to execution of arbitrary code with the context of the user running the ExifTool. Note: This strike exploits GitLab CE which runs the ExifTool internally. GitLab also identifies this same vulnerability with CVE-2021-22205.
Strike GitLab Community and Enterprise Edition Remote Command Execution	CWE: 94 CVE: 2021-22205	This strike exploits a remote code execution vulnerability in GitLab Community and Enterprise Editions. This vulnerability is due to improper validation of image files that are passed to file parser. A remote, authenticated attacker could exploit this vulnerability by sending specially crafted image file to an unspecified endpoint. Successfully exploiting this vulnerability could result in remote command execution on the target system.
Strike Micro Focus Operation Bridge Reporter LogonResource OS Command Injection	CWE: 78 CVE: 2021-22502	This strike exploits an OS Command Injection Vulnerability in Micro Focus OBR. The vulnerability is due to improper sanitization of username parameter. A remote, unauthenticated attacker can exploit this vulnerability by sending crafted http requests containing shell metacharacters to the LogonResource endpoint. Successful exploitation of this vulnerability could lead to remote code execution.

Name	References	Description
Strike Advantech iView CommandServlet Directory Traversal Vulnerability	CVE: 2021-22656	This strike exploits a directory traversal vulnerability in Advantech iView. The vulnerability arises from improper validation of user-supplied input in the CommandServlet Java class. A remote, unauthenticated attacker could leverage this flaw by sending crafted HTTP requests, potentially leading to the disclosure of sensitive files and information on the server.
Strike Advantech iView UserServlet SQL Injection	CWE: 89 CVE: 2021-22658	This strike exploits a SQL injection vulnerability in Advantech iView. The vulnerability is due to improper validation of user-supplied input when processing the request in UserServlet Java class. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in the execution of arbitrary SQL statement on the target server.
Strike Schneider Electric Struxureware Data Center Expert Command Injection Vulnerability	CVE: 2021-22795	This strike exploits a command injection vulnerability in Schneider Electric Struxureware Data Center Expert. The vulnerability exists due to improper sanitization of the "config" parameter in HTTP POST requests to the "/nbc/compress/repository/test" endpoint. A remote, authenticated attacker could leverage this flaw to execute arbitrary commands on the system with root privileges.
Strike Citrix ShareFile Storage Zones Controller NeatUpload Directory Traversal	CVE: 2021-22941 CWE: 284	The vulnerability allows remote attackers to save files to an arbitrary file path under the web root directory in the NeatUpload library of Citrix ShareFile Storage Zones Controller due to improper validation of an ID parameter in file upload requests. Successful exploitation could result in the execution of arbitrary code on the target server.
Strike F5 BIG-IP and BIG-IQ iControl REST Code Execution	CWE: 284 CVE: 2021-22986	This strike exploits an authentication bypass vulnerability in F5 BIG-IP and BIG-IQ products. The vulnerability is due to improper handling of user-supplied authentication token and the loginReference link in HTTP requests. A remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the server. A successful attack may result in remote code execution in the security context of ROOT.
Strike Joomla mod_breadcrumbs Title Store Cross-Site Scripting	CWE: 79 CVE: 2021-23124	This strike exploits a cross-site scripting vulnerability in Joomla CMS. This vulnerability is due to inadequate input filtering in the title attribute of mod_breadcrumbs. Successful exploitation could result in arbitrary script code being executed in the security context of the browser.
Strike Oracle Business Intelligence BIRemotingServlet Insecure Deserialization Vulnerability	CVE: 2021-2456	This strike exploits an insecure deserialization vulnerability in Oracle Business Intelligence. The vulnerability arises from improper validation of AMF3 objects in requests to the BIRemotingServlet. A remote attacker can leverage this flaw by sending specially crafted AMF packets, leading to arbitrary code execution in the context of the affected server.

Name	References	Description
Strike SaltStack Salt salt wheel pillar_roots write Method Directory Traversal	CWE: 22 CVE: 2021-25282	This strike exploits a directory traversal vulnerability that exists in the WheelClient for Salt API, a component of SaltStack Salt. The vulnerability is due to improper validation of user-supplied input in the pillar_roots.write method. A remote attacker could exploit this vulnerability by sending a crafted HTTP request to the targeted server. Successful exploitation can result in arbitrary file creation and, in the worst case, remote code execution in the context of the root user.
Strike Nagios XI Configwizards Windowswmi Command Injection	CWE: 78 CVE: 2021-25296	This strike exploits a command injection vulnerability in Nagios XI 5.7.5. The vulnerability is due to insufficient input validation of the requests submitted to the Windowswmi.inc.php file. A remote authenticated attacker can exploit this vulnerability by sending a crafted request to the server. Successful exploitation could result in arbitrary command execution with privileges of the web server running on the target system. NOTE - The strike has one-arm support where it tries to connect to a netcat listener with a bash shell running on port 4444 on the vulnerable webserver (Creds - nagiosadmin/1234) itself.
Strike Nagios XI Configwizards Switch Command Injection	CWE: 78 CVE: 2021-25297	This strike exploits a command injection vulnerability in Nagios XI version xi-5.7.5. The vulnerability exists in the file /usr/local/nagiosxi/html/includes/configwizards/switch/switch.inc.php due to improper sanitization of authenticated user-controlled input by a single HTTP request, which can lead to OS command injection on the Nagios XI server. NOTE - The strike has one-arm support where it tries to connect to a netcat listener with a bash shell running on port 4444 on the vulnerable webserver (Creds - nagiosadmin/1234) itself.
Strike Nagios XI Configwizards Cloud-vm Command Injection	CWE: 78 CVE: 2021-25298	This strike exploits a command injection vulnerability in Nagios XI 5.7.5. The vulnerability is due to insufficient input validation of the requests submitted to the Cloud-vm.inc.php file. A remote authenticated attacker can exploit this vulnerability by sending a crafted request to the server. Successful exploitation could result in arbitrary command execution with privileges of the web server running on the target system. NOTE - The strike has one-arm support where it tries to connect to a netcat listener with a bash shell running on port 4444 on the vulnerable webserver (Creds - nagiosadmin/1234) itself.
Strike Nagios XI Web SSH Terminal sshterm Cross-Site Scripting	CWE: 79 CVE: 2021-25299	This strike exploits a cross-site scripting vulnerability in Nagios XI 5.7.5 . This vulnerability is due to improper validation of the url parameter in sshterm.php while accessing the web SSH terminal.A remote attacker can exploit this vulnerability by enticing the user to visit a specially crafted link or page. Successful exploitation could result in arbitrary script code being executed in the security context of the browser.
Strike Apache Druid Remote Code Execution	CWE: 502 CVE: 2021-25646	This strike exploits a deserialization vulnerability in Apache Druid. The vulnerability is due to improper deserialization of a JSON data into Java objects. A remote, unauthenticated attacker could exploit this vulnerability by submitting a specially crafted JSON file which could result in arbitrary command execution.

Name	References	Description
Strike Atlassian Confluence OGNL Remote Code Execution	CWE: 74 CVE: 2021-26084	This strike exploits an OGNL injection vulnerability in the createpage-entervariables resource of Confluence Server and Data Center. The vulnerability is due to improper validation of a parameter in a HTTP POST request. To exploit this vulnerability, a remote, unauthenticated attacker can submit a request with encoded single quote in order to perform an OGNL injection attack. A successful attack can result in arbitrary command execution in the context of the server process.
Strike Atlassian Confluence Information Disclosure	CWE: 862 CVE: 2021-26085	This strike exploits an information disclosure vulnerability in Atlassian Confluence. The vulnerability is due to improper path validation. A remote, unauthenticated attacker could exploit this vulnerability by submitting a specially crafted HTTP request which could result in arbitrary file read.
Strike CMS Made Simple Server-Side Template Injection Vulnerability	CVE: 2021-26120	This strike exploits a server-side template injection vulnerability in CMS Made Simple. The vulnerability exists due to improper validation of user-supplied input in the "name" parameter of the "{function}" tag within the Smarty template engine. A remote, authenticated attacker could leverage this flaw to execute arbitrary code on the affected system, potentially gaining full control over the server.
Strike Microsoft Internet Explorer 9-11 MSHTML Remote Code Execution	CVE: 2021-26411 CWE: 119	This strike exploits a memory corruption vulnerability in the Microsoft Internet Explorer 9 and 11 browsers. The vulnerability is due to improper use of memory in the MSHTML library. An attacker could exploit this vulnerability by convincing a user to open a malicious HTML page, which could lead to remote code execution.
Strike Microsoft Exchange New-DlpPolicy Cmdlet Remote Code Execution Vulnerability	CVE: 2021-26412	This strike targets a remote code execution vulnerability in Microsoft Exchange Server. The issue arises from improper validation of the "commandBlock" tag in DLP policy templates when processing the "ruleParameters" tag. Exploiting this flaw allows an authenticated attacker to execute arbitrary commands with SYSTEM privileges on the affected server.
Strike Microsoft Exchange ProxyLogon Server Side Request Forgery	CVE: 2021-26855 CWE: 918	A server side request forgery exists in multiple versions of Microsoft Exchange Server. The vulnerability resides in 'Microsoft.Exchange.FrontEndHttpProxy.dll' and is due to improper validation of requests for static resources sent to the backend component of the server. A remote unauthenticated attacker may send an HTTP POST request with a crafted 'Cookie' header to access resources that are otherwise accessible only for administrative users.
Strike Microsoft Exchange Server Arbitrary File Write	CWE: 23 CVE: 2021-26858	This strike exploits a path traversal vulnerability which affects Microsoft Exchange Server. The vulnerability is due to insufficient validation of the user provided path. A remote, authenticated attacker can exploit this vulnerability by sending several crafted requests to the target system. Successful exploitation results in remote code execution under the security context as SYSTEM.

Name	References	Description
Strike Apache Druid JDBC Connection Remote Code Execution	CWE: 15 CVE: 2021-26919	This strike exploits a deserialization vulnerability in Apache Druid. The vulnerability is due to missing validation on allowed JDBC connection properties. A remote, unauthenticated attacker could exploit this vulnerability by submitting a crafted JDBC connection URL in a MySQL datasource. Note: This strike contains just the configuration request to the Apache Druid server. This request is used to enforce the Apache Druid to connect to a MySQL server, request some data and deserialize it. The MySQL connection generated by this request is not part of this strike.
Strike Microsoft Exchange FilePathName Arbitrary File Write	CVE: 2021-27065 CWE: 73 EXPLOITDB : 49637	An arbitrary file upload vulnerability exists in Microsoft Exchange Server due to lack of sanitization of 'FilePathName' parameter in Virtual Directory reset requests. A remote authenticated attacker may send crafted JSON HTTP requests to upload a webshell on the target system and execute arbitrary commands as the SYSTEM user.
Strike Netgear ProSAFE NMS300 Arbitrary File Deletion Vulnerability	CVE: 2021-27272	This strike exploits an arbitrary file deletion vulnerability in Netgear ProSAFE NMS300. The vulnerability resides in the ReportTemplateController class, specifically in the clear() method, which fails to properly sanitize directory traversal characters in the path parameter. A remote authenticated attacker could leverage this flaw by sending crafted HTTP requests to delete arbitrary files on the server, potentially leading to denial-of-service conditions.
Strike Netgear ProSAFE NMS300 Post-Authentication Command Injection Vulnerability	CVE: 2021-27273	This strike exploits a command injection vulnerability in Netgear ProSAFE NMS300. The vulnerability exists due to insufficient validation of the "fileName" parameter in the rebootSystem() method of the SettingConfigController class. A remote, authenticated attacker could leverage this flaw by sending specially crafted HTTP requests, leading to the execution of arbitrary commands with SYSTEM privileges.
Strike Netgear ProSAFE NMS300 Unrestricted File Upload Vulnerability	CVE: 2021-27274	This strike exploits an unrestricted file upload vulnerability in Netgear ProSAFE NMS300. The vulnerability resides in the MFileUploadController class, specifically in the uploadFile() method, which fails to properly validate the file type and parameters of uploaded files. A remote attacker could exploit this vulnerability by uploading a malicious file, leading to arbitrary code execution under the security context of SYSTEM.
Strike Yealink Device Management Server-Side Request Forgery	CWE: 78 CVE: 2021-27561	This strike exploits a Server-Side Request Forgery Vulnerability in Yealink Device Management. This vulnerability lies in the /sm/api/v1/firewall/zone/services URI. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation of this vulnerability could lead to command execution in the context of the root user.
Strike Apache Solr ReplicationHandler SSRF Vulnerability	CVE: 2021-27905	This strike exploits a server-side request forgery vulnerability in Apache Solr. The vulnerability is located in the ReplicationHandler's handling of the masterUrl and leaderUrl parameters. Exploiting this vulnerability allows a remote attacker to perform arbitrary file writes, disclose sensitive information, and spoof server conditions.

Name	References	Description
Strike Apache Superset Markdown Component Stored Cross-Site Scripting	CWE: 79 CVE: 2021-27907	This strike exploits a stored cross-site scripting vulnerability in the Markdown component of Apache Superset. This vulnerability is due to insufficient validation of Markdown snippet in a dashboard. A remote authenticated attacker can exploit this vulnerability by sending crafted requests to the target server. Successful exploitation could result in arbitrary script execution in the target user's browser.
Strike Apache OFBiz SOAPService XMLRPC Insecure Deserialization	CVE: 2021-29200 CWE: 502	This strike exploits an insecure deserialization vulnerability in Apache OFBiz. The vulnerability is a result of insufficient validation of XML-RPC requests in the UtilObject class. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to a vulnerable server. Successful exploitation can lead to remote code execution, in the context of the user running the server.
Strike Alibaba Nacos AuthFilter Authentication Bypass Vulnerability	CVE: 2021-29441	This strike exploits an authentication bypass vulnerability in Alibaba Nacos. The vulnerability is located in the AuthFilter servlet filter implementation, specifically in the doFilter method of the AuthFilter class. Exploiting this vulnerability allows a remote, unauthenticated attacker to gain unauthorized access to endpoints that typically require authentication.
Strike Ivanti Avalanche imagePath Directory Traversal Vulnerability	CVE: 2021-30497	This strike exploits a directory traversal vulnerability in Ivanti Avalanche. The vulnerability resides in the improper validation of the "imageFilePath" parameter in HTTP requests. A remote, unauthenticated attacker could leverage this flaw to access arbitrary files on the server, potentially leading to the disclosure of sensitive information.
Strike Microsoft HTTP.sys UlpParseAcceptEncoding Remote Code Execution Vulnerability	CWE: 416 CVE: 2021-31166	A use-after-free vulnerability exists in the HTTP Protocol Stack HTTP.sys for Microsoft Internet Information Services. The vulnerability is due to a design weakness in the UlpParseAcceptEncoding method. This vulnerability can be exploited by a remote, unauthenticated attacker by sending a crafted Accept-Encoding header in an HTTP request to the target server. Successful exploitation could lead to remote code execution with kernel privileges or to a denial of service.
Strike Microsoft Exchange MailboxExportRequest Arbitrary File Write	CWE: 22 CVE: 2021-31207	This strike exploits an arbitrary file write vulnerability in Microsoft Exchange. The vulnerability is due to improper handling of MailboxExportRequest commands. An authenticated, remote attacker can exploit this vulnerability by sending a crafted MailboxExportRequest command to the target server. Successful exploitation could result in the writing of an arbitrary file which may be used to facilitate the execution of arbitrary code.
Strike Laravel Ignition Solutions Remote Code Execution	CVE: 2021-3129 CWE: 94	This strike exploits a file upload vulnerability in Laravel Ignition. The issue arises because of the insecure usage of file_get_contents() and file_put_contents() present in the Ignition module. This allows an attacker to inject malicious scripts in the viewFile parameter of the solutions present in the Ignition module. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted request to the target server. Successful exploitation can lead to arbitrary code execution.

Name	References	Description
Strike WebSVN Search.php Command Injection Vulnerability	CVE: 2021-32305	This strike exploits a command injection vulnerability in WebSVN. The vulnerability exists due to improper sanitization of the "search" parameter in requests sent to the search.php endpoint. A remote, unauthenticated attacker can leverage this flaw to execute arbitrary commands with the privileges of the web server on the target system.
Strike SmartStoreNET ForumPost Stored Cross-Site Scripting Vulnerability	CVE: 2021-32608	This strike exploits a stored cross-site scripting vulnerability in SmartStoreNET. The vulnerability resides in the improper handling of BBCode url tags within forum posts. A remote attacker could exploit this flaw by posting maliciously crafted forum messages, leading to arbitrary script execution in the browser of users viewing the affected pages.
Strike Studio-42 elFinder Archive Command Injection Vulnerability	CVE: 2021-32682	This strike exploits a command injection vulnerability in Studio-42 elFinder. The vulnerability resides in the insufficient validation of the "name" parameter when creating an archive in the makeArchive function. A remote, unauthenticated attacker can leverage this flaw to execute arbitrary commands with the privileges of the web server process.
Strike WooCommerce Blocks WordPress Plugin SQL Injection Vulnerability	CVE: 2021-32789	This strike exploits an SQL injection vulnerability in the WooCommerce Blocks WordPress plugin. The vulnerability arises from insufficient input validation in the "calculate_attribute_counts" parameter of the "/wc/store/products/collection-data" API endpoint. A remote, unauthenticated attacker can exploit this flaw by sending crafted HTTP requests, leading to the execution of arbitrary SQL SELECT queries and unauthorized retrieval of database information.
Strike Delta Industrial Automation DIAEnergie Arbitrary File Upload Vulnerability	CVE: 2021-32955	This strike exploits an arbitrary file upload vulnerability in Delta Industrial Automation DIAEnergie. The vulnerability resides in the HandlerPage_KID endpoint due to insufficient input validation on the HtmlId parameter and lack of authentication. A remote, unauthenticated attacker could leverage this flaw to upload malicious files, potentially leading to arbitrary code execution on the server.
Strike Microsoft Exchange ProxyShell EwsAutodiscoverProxyRequestHandler SSRF Auth Bypass	CWE: 918 CVE: 2021-34473	This strike exploits a server side request forgery (SSRF) vulnerability in the EwsAutodiscoverProxyRequestHandler component of Microsoft Exchange. The vulnerability is due to insufficient handling of explicit logon requests to the autodiscover component of Exchange. An unauthenticated, remote attacker can exploit this vulnerability by sending a crafted request to the vulnerable Exchange server. Successful exploitation results in requests being made to backend servers with administrative privileges without any need of authentication. *NOTE: In OneArm mode, the strike makes requests for enumerating email addresses, Server ID , Legacy DN and saves a draft email with a file attachment with SID 'S-1-5-21-1943555408-1405878097-3563671238-500'.
Strike Microsoft Exchange Proxyshell PowerShell Backend Privesc	CWE: 287 CVE: 2021-34523	This strike exploits a privilege escalation vulnerability in the PowerShell remoting feature of Microsoft Exchange. The vulnerability is due to improperly deserializing access token provided in the request. A remote authenticated attacker can provide the access token for an user (including the Exchange Admin user) as part of X-Rps-CAT query in the request resulting in to run powershell commands impersonating the that user.

Name	References	Description
Strike Foxit Reader and Editor Use-After-Free Vulnerability in Annotation Handling	CVE: 2021-34833	This strike exploits a use-after-free vulnerability in Foxit PDF Reader and Editor. The vulnerability resides in the improper handling of the author property of Annotation objects within JavaScript. Exploiting this flaw allows a remote attacker to execute arbitrary code by enticing a user to open a maliciously crafted PDF file.
Strike Realtek SDK Management Web Interface Vulnerabilities	CVE: 2021-35395 CWE: 77	This strike exploits multiple vulnerabilities in the Realtek SDK Management Web Interface. The vulnerabilities are due to improper validation of user supplied input and might result in remote code execution. A remote, unauthenticated attacker might exploit this vulnerability by sending a crafted HTTP message to the targeted device. Note: This strike exploits the vulnerability in formSysCmd and formWsc endpoints.
Strike ForgeRock Access management Insecure Deserialization	CWE: 502 CVE: 2021-35464	An insecure deserialization vulnerability exists in ForgeRock Access Management and OpenAM. The vulnerability is due to insufficient validation of user-supplied data. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request. Successful exploitation results in full control of the target server.
Strike Oracle Access Manager OpenSSO Agent Insecure Deserialization	CWE: 502 CVE: 2021-35587	This strike exploits an insecure deserialization vulnerability in Oracle Access Manager. The vulnerability is due to insufficient validation of requests sent to the OpenSSO Agent endpoint. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to a vulnerable server. Successful exploitation can result in arbitrary code execution under the security context of the affected server.
Strike Hikvision Improper Input Validation	CWE: 78 CVE: 2021-36260	This strike exploits a command injection vulnerability in Hikvision IP camera/NVR firmware. The vulnerability is due to the insufficient input validation. It inserts a command into an XML payload used with an HTTP PUT request sent to the '/SDK/webLanguage' endpoint, resulting in command execution as the root user. A remote, unauthenticated attacker could exploit the vulnerability to launch a command injection attack by sending some messages with malicious commands.
Strike Sunhillo SureLine OS Command Injection Vulnerability	CWE: 78 CVE: 2021-36380	This strike exploits an OS command injection vulnerability in Sunhillo SureLine. The vulnerability is caused by improper input sanitization in the /cgi/networkDiag.cgi script, which allows attackers to execute arbitrary commands with root privileges. By manipulating user-controllable parameters ipAddr or dnsAddr, remote unauthenticated attackers can inject OS commands. Successful exploitation could lead to remote code execution on the target server.
Strike Nagios XI Post-auth RCE through Path Traversal	CWE: 22 CVE: 2021-37343	This strike exploits a path traversal vulnerability in Nagios XI versions prior to 5.8.5 . This vulnerability is due to improper validation of the job parameter in autodiscovery feature. A remote authenticated attacker can exploit this vulnerability by sending a crafted request. Successful exploitation could result in arbitrary file creation and further more can result in arbitrary code being executed in the context of the web server. Note: This strike contains just the authentication and the request required to create a backdoor in the web server.

Name	References	Description
Strike Nagios XI Post-auth SQL Injection	CWE: 89 CVE: 2021-37350	This strike exploits a SQL Injection vulnerability in Nagios XI versions prior to 5.8.5. This vulnerability is due to improper validation of the field_value parameter in the bulkmodifications component. A remote authenticated attacker can exploit this vulnerability by sending a crafted request. Successful exploitation could allow an attacker to execute SQL commands on the target server.
Strike Zoho ManageEngine ServiceDesk Authentication Bypass Vulnerability	CWE: 306 CVE: 2021-37415	This strike exploits an authentication bypass vulnerability in the Zoho ServiceDesk Plus, in the REST API URLs on all versions prior to 11306. This vulnerability is due to an error in normalizing REST API URLs before applying security filtering against defined URI path patterns, bypassing security filters. Successful exploitation allows an attacker to send a crafted request to ServiceDesk Plus, which gets processed without any authentication.
Strike Centreon ProceduresProxy.class.php SQL Injection Vulnerability	CVE: 2021-37558	This strike exploits an SQL injection vulnerability in the Centreon web application. The vulnerability is located in the ProceduresProxy.class.php file, specifically within the getHostId() and getServiceId() functions, which fail to properly sanitize the host_name and service_description parameters. Exploiting this vulnerability allows a remote, unauthenticated attacker to execute arbitrary SQL commands on the database, potentially leading to unauthorized data manipulation or further compromise of the target system.
Strike Zoho ManageEngine ADManager Plus Unrestricted File Upload Vulnerability cve_2021_37921	CVE: 2021-37921	This strike targets an unrestricted file upload vulnerability in Zoho ManageEngine ADManager Plus. The issue arises from insufficient validation of uploaded files in the ReportsAction class. Exploiting this flaw allows a remote authenticated attacker to upload arbitrary files, potentially leading to remote code execution with SYSTEM privileges.
Strike Zoho ManageEngine ADManager Plus Unrestricted File Upload Vulnerability cve_2021_37926	CVE: 2021-37926	This strike exploits an unrestricted file upload vulnerability in Zoho ManageEngine ADManager Plus. The vulnerability exists due to insufficient validation of file types in the LicenseAction class when handling uploaded files. A remote authenticated attacker can leverage this flaw to upload malicious files, potentially leading to remote code execution with SYSTEM-level privileges.
Strike Google Chrome Hole Memory Corruption	CWE: 755 CVE: 2021-38003	This strike exploits a vulnerability in the V8 in Google Chrome. The vulnerability exists due to improper handling of the internal TheHole value when an exception occurs during execution. By crafting specific inputs, it is possible to trigger a scenario where TheHole leaks into JavaScript code. Successful exploitation could result in memory corruption.
Strike Microsoft Azure Open Management Infrastructure Authentication Bypass	CWE: 305 CVE: 2021-38647	This strike exploits an authentication bypass vulnerability in Microsoft Azure Open Management Infrastructure. The vulnerability is due to improper validation of the Authorization header in the HTTP request supplied. A remote attacker could exploit this vulnerability by sending a crafted request to a vulnerable server. A successful attack might result in the remote code execution in the context of root user.

Name	References	Description
Strike VMware NSX Manager XStream Remote Code Execution Vulnerability	CWE: 502 CVE: 2021-39144	This strike exploits an insecure deserialization vulnerability in the XStream library in VMWare NSX Manager. This flaw, originally identified as an XStream deserialization issue, leverages the application's XML processing to execute arbitrary code. Due to inadequate input validation in XStream, the application deserializes untrusted XML data insecurely. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted XML payload to an unauthenticated API endpoint. Successful exploitation could allow the attacker to execute code with elevated privileges, potentially leading to full system compromise.
Strike Grafana Labs Grafana Snapshot Authentication Bypass	CWE: 287 CVE: 2021-39226	This strike exploits an Authentication Bypass vulnerability in Grafana. The vulnerability is due to insufficient authorization on web endpoints - "/api/snapshots" and "/api/snapshots-delete". A remote, unauthenticated attacker can exploit the vulnerability by sending a request to one of the affected endpoints. Successful exploitation could result in disclosure of existing snapshots and deletion of application snapshots. *NOTE: While running this strike in OneArm mode, it sends a crafted request to the target server where the current snapshot can be viewed and the same can also be deleted.
Strike Nagios XI Custom Includes Component Arbitrary File Upload Vulnerability	CVE: 2021-40344	This strike exploits an arbitrary file upload vulnerability in the Custom Includes component of Nagios XI. The vulnerability resides in the misconfiguration of the .htaccess file within the /images subdirectory of the component. A remote, authenticated attacker can leverage this flaw to upload and execute malicious PHP code, potentially leading to arbitrary code execution under the web server's security context.
Strike Nagios XI cmdsubsys.php Command Injection Vulnerability	CVE: 2021-40345	This strike targets a command injection vulnerability in the cmdsubsys.php script of Nagios XI. The issue arises from improper sanitization of user-supplied input in the names of files within uploaded Zip archives. Exploiting this flaw allows a remote, authenticated attacker to execute arbitrary commands with the privileges of the nagios user.
Strike Apache httpd mod_proxy unix socket path SSRF	CWE: 918 CVE: 2021-40438	This strike exploits a Server Side Request Forgery (SSRF) vulnerability in Apache mod_proxy component. The vulnerability is due to a missing validation of the unix socket path in an HTTP request. A remote attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in target server sending requests to internal servers leading to information disclosure. *NOTE: When running this strike in OneArm mode, due to SSRF, the target server will attempt to send a HTTP GET request to the IP address 192.168.2.7 and port 8081.
Strike Zoho ManageEngine ADSelfService Plus Authentication Bypass	CWE: 287 CVE: 2021-40539	This strike exploits an authentication bypass vulnerability in Zoho ManageEngine ADSelfService Plus. The vulnerability is due to an error in normalizing the URLs before validation. A remote attacker could exploit this vulnerability by sending crafted requests to the target server. Successful exploitation could allow the attacker to bypass authentication and exploit endpoints to perform subsequent attacks leading to arbitrary command execution. *NOTE: The strike attempts to perform authentication bypass and call random endpoints which usually requires authentication.

Name	References	Description
Strike Aviatrix Controller Unrestricted File Upload	CVE: 2021-40870 CWE: 23	This strike exploits a file upload vulnerability in Aviatrix Controller. The vulnerability allows unauthenticated attackers to upload malicious files, which can then be exploited via directory traversal to execute arbitrary code. Successful exploitation of this vulnerability allows remote attackers to execute arbitrary commands on the affected system.
Strike Metabase GeoJSON API Local File Inclusion Vulnerability	CVE: 2021-41277 CWE: 22	This strike exploits a local file inclusion vulnerability in Metabase GeoJSON API. The vulnerability is due to insufficient validation of url. A remote unauthenticated attacker can exploit this vulnerability by specially crafted HTTP GET request. Successful exploitation of this vulnerability could lead to information disclosure, file exposure and environment variables to unauthenticated users.
Strike Netgate pfSense diag_routes.php Command Injection Vulnerability	CVE: 2021-41282	This strike exploits a command injection vulnerability in Netgate pfSense. The vulnerability resides in the diag_routes.php file due to insufficient validation of user-supplied input in the filter parameter. A remote, authenticated attacker can leverage this flaw to execute arbitrary operating system commands, potentially leading to full system compromise.
Strike Apache HTTP Server Path Traversal	CWE: 22 CVE: 2021-41773	This strike exploits a Path Traversal vulnerability in Apache HTTP server prior to 2.4.50. This vulnerability is due to improper validation of path in the CGI extension. A remote attacker can exploit this vulnerability by sending a crafted request. Successful exploitation could allow an attacker to execute arbitrary commands on the target server. Note: In order to exploit this vulnerability the Apache HTTP server needs to have CGI extension enabled and granted permission for root folder.
Strike Apache httpd ap_normalize_path Directory Traversal	CWE: 22 CVE: 2021-42013	This strike exploits a directory traversal vulnerability in Apache httpd. The vulnerability is due to improper normalization of paths in the request URI. This vulnerability is due to incomplete fix of CVE-2021-41773. A remote, unauthenticated attacker could exploit the vulnerability by sending crafted HTTP requests to a target server configured with the exploitable configurations. Successful exploitation could result in execution of arbitrary code under the security context of the server process. *NOTE: When ran in OneArm mode, the strike will attempt to create a file in /tmp using /bin/bash
Strike Ivanti Avalanche Central FileStore Command Injection Vulnerability	CVE: 2021-42129	This strike exploits a command injection vulnerability in Ivanti Avalanche Enterprise Service. The vulnerability exists due to insufficient validation of input fields in the Central FileStore configuration settings. A remote, authenticated attacker could leverage this flaw by sending crafted requests, leading to the execution of arbitrary commands on the server with SYSTEM privileges.
Strike Sitecore XP Report.ashx Insecure Deserialization	CWE: 502 CVE: 2021-42237	This strike exploits an insecure deserialization vulnerability in Sitecore XP. This vulnerability is due to insufficient validation of serialized data sent to Report.ashx. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in arbitrary code execution within the security context of the user running the vulnerable application.

Name	References	Description
Strike BQE BillQuick Web Suite Login Page SQL Injection	CWE: 89 CVE: 2021-42258	This strike exploits a SQL injection vulnerability in BQE BillQuick web suite. The vulnerability is due to improper validation of user-supplied input when processing the login request. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in the execution of arbitrary SQL statement on the target server.
Strike Adobe RoboHelp Server fileName Directory Traversal	CWE: 78 CVE: 2021-42727	This strike exploits a directory traversal vulnerability in Adobe RoboHelp Server. When processing the fileName parameter, there is an input validation error that leads to this vulnerability. A remote authenticated attacker can exploit this vulnerability by sending crafted messages to the server. Successful exploitation could achieve arbitrary code execution with privileges of SYSTEM.
Strike Zoho ManageEngine Network Configuration Manager Ping Command Injection	CWE: 77 CVE: 2021-43319	This strike exploits a command injection vulnerability in Zoho ManageEngine Network Configuration Manager. The vulnerability is due to insufficient validation in the ipAddress field of the ping functionality in add device web interface. A remote, authenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could lead to arbitrary code execution in the security context of the web server. *Note : Upon running the strike in one-arm mode a file named Test is created in /tmp directory of the vulnerable server. The default credentials being used are admin/admin.
Strike FusionPBX fax_send.php Command Injection Vulnerability	CVE: 2021-43405	This strike exploits a command injection vulnerability in the fax_send.php script of FusionPBX. The vulnerability exists due to insufficient input validation of the fax_extension parameter in HTTP requests. Exploiting this flaw allows a remote, authenticated attacker to execute arbitrary system commands with the privileges of the server process.
Strike Grafana Plugin Directory Traversal	CWE: 22 CVE: 2021-43798	This strike exploits a directory traversal vulnerability in Grafana. The vulnerability is due to improper sanitization for the plugin assets route. A remote, unauthenticated attacker could exploit the vulnerability by sending crafted HTTP requests to a target server. Successful exploitation can result in arbitrary file read in the context of the Grafana user.
Strike Roundcube Webmail SQL Injection Vulnerability	CWE: 89 CVE: 2021-44026	This strike exploits an SQL injection vulnerability in Roundcube. The vulnerability is due to insufficient validation of user-provided search_params data. To execute the attack, the malicious actor must first authenticate within a Roundcube session. Upon successful exploitation, the attacker could read sensitive information, modify database content, or escalate privileges based on the permissions granted to the database account that Roundcube utilizes.
Strike Zoho ManageEngine ImportTechniciansAction Arbitrary File Upload	CWE: 287 CVE: 2021-44077	This strike exploits an arbitrary file write vulnerability that has been reported in Zoho ManageEngine ServiceDesk Plus, ServiceDesk Plus MSP, and SupportCenter Plus. The vulnerability is due to insufficient validation of input data. An unauthenticated remote attacker can exploit this vulnerability by submitting a crafted request to the target server. Successful exploitation results in the writing of an arbitrary file to the target application, potentially leading to execution of arbitrary code as SYSTEM.

Name	References	Description
Strike Apache httpd mod_proxy Null Pointer Dereference DoS	CWE: 476 CVE: 2021-44224	A denial of service vulnerability exists in multiple versions of Apache Software Foundation httpd prior to 2.4.52. The flaw is due to improper handling of malformed Request-URIs requests. An unauthenticated remote attacker may send a crafted request to the target server. Successful exploitation could result in a denial of service (DoS) condition.
Strike Apache Log4j JndiManager JNDI Injection RCE LDAP	CWE: 20 CVE: 2021-44228	A JNDI Injection vulnerability exists in Apache Log4j versions 2.0 - 2.14. The vulnerability is due to improper handling of logged messages in the JndiManager class. By sending a crafted message to be logged by the target application, a remote unauthenticated attacker may execute arbitrary code on the target system. *NOTE: When running this strike in OneArm mode, the attacker will send a request to make the vulnerable server attempt to make a LDAP request to a JNDI server running on 192.168.2.7 port 1389 to retrieve the serialized object which will execute mktemp command.
Strike Zoho Desktop Central Authentication Bypass Vulnerability	CWE: 287 CVE: 2021-44515	This strike exploits an authentication bypass vulnerability in ManageEngine Desktop Central. The vulnerability is due to an input validation error in the StateFilter class. A remote, unauthenticated attacker could bypass the authentication of the console component and then send commands via WebSockets to the managed devices by the ManageEngine Desktop Central server. This may potentially cause remote code execution, allowing a malicious, unauthenticated attacker to execute arbitrary code on the devices managed by the ManageEngine Desktop Central server.
Strike Ivanti EPM Cloud Services Appliance Code Injection Vulnerability	CWE: 94 CVE: 2021-44529	This strike exploits a command injection vulnerability in the Ivanti Cloud Services Appliance (CSA) for Ivanti Endpoint Manager. The vulnerability is due to insufficient input validation and improper handling of cookie data. The vulnerable code allows an unauthenticated attacker to inject and execute arbitrary PHP code by crafting specific cookie headers, leading to execution of base64-encoded payloads via the eval() function. Successful exploitation results in command execution as the 'nobody' user.
Strike Apache httpd mod_lua Integer Underflow	CWE: 191 CVE: 2021-44790	A integer underflow vulnerability exists in multiple versions of Apache Software Foundation httpd prior to 2.4.52. The flaw is due to improper handling of the request body. An unauthenticated remote attacker may sent a crafted request to the target server. Successful exploitation could result in remote code execution or denial of service condition. * Target Apached server must have the mod_lua module enabled and have the lua-script handler set for Lua scripts stored on the server. * The target must contain a Lua script utilizing the r:parsebody() function.
Strike Apache Log4j JndiManager JNDI Injection RCE	CWE: 610 CVE: 2021-45046	A JNDI Injection vulnerability exists in Apache Log4j version 2.0-beta9 to 2.15.0, excluding 2.12.2. The vulnerability is due to improper handling of logged messages when the logging configuration uses a non-default Pattern Layout. An attacker who can control an item in the MapMessage or StrucutredDataMessage can exploit this vulnerability by sending a crafted message to be logged by the target application, a remote unauthenticated attacker can cause denial of service or in certain configuration execute arbitrary code on the target system. This vulnerability is due to the incomplete fix for CVE-2021-44228. *NOTE: This strike uses the local hostname check bypass method.

Name	References	Description
Strike Apache Log4j StrSubstitutor Uncontrolled Recursion Denial of Service	CWE: 674 CVE: 2021-45105	An uncontrolled recursion from self-referential lookups exists in Apache Log4j version 2.0-alpha1 through 2.16.0 (excluding 2.12.3 and 2.3.1). An attacker who can control an item in Thread Context Map can exploit this vulnerability by sending a crafted message to be logged by the target application, a remote unauthenticated attacker can cause denial of service by sending a crafted message.
Strike D Link Multiple Routers Remote Code Execution Vulnerability	CVE: 2021-45382 CWE: 78	This strike exploits an OS command injection vulnerability in D-Link Routers. The vulnerability is due to insufficient validation of user supplied input. An unauthenticated attacker could exploit this vulnerability by sending a crafted HTTP request and might result in remote code execution.
Strike WordPress Photo Gallery Plugin SQL Injection Vulnerability	CVE: 2022-0169	This strike exploits a SQL injection vulnerability in the WordPress Photo Gallery plugin. The vulnerability arises from improper sanitization of the `bwg_tag_id_bwg_thumbnails_0` parameter in HTTP requests. A remote, unauthenticated attacker can leverage this flaw to execute arbitrary SQL commands on the database, potentially leading to data exfiltration or unauthorized access.
Strike Sophos Firewall User Portal and Webadmin Authentication Bypass	CWE: 287 CVE: 2022-1040	This strike exploits an Authentication Bypass vulnerability in Sophos Firewall. The vulnerability is due to insufficient sanitization of null characters in the "json" parameter sent to the Controller endpoint. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successfully exploiting this vulnerability could result in access control policy bypass and remote code execution at worst. *NOTE: When running this strike in OneArm mode, it sends a crafted request to the target server on port 4444 for webadmin or on port 443 for userportal. Due to Authentication Bypass, the target server responds with a valid session cookie for the username in the request.
Strike Google Chrome defineProperty Improper Interceptor Handling	CWE: 843 CVE: 2022-1232 GOOGLE: 2280	This strike exploits a vulnerability in Google Chrome. Specifically, javascript can be crafted in such a way that when an Object replaces a property store an interceptor is encountered that causes memory corruption. When this happens a denial of service condition, or potentially remote code execution, may occur.
Strike F5 BIG-IP iControl REST Authentication Bypass	CWE: 306 CVE: 2022-1388	This strike exploits an authentication bypass vulnerability in F5 BIG-IP product. The vulnerability is due to improper handling of requests sent to management port. A remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the management port. A successful attack may result in remote code execution in the security context of ROOT.

Name	References	Description
Strike Keysight N6854A and N6841A RF Sensor Insecure Deserialization	CWE: 502 CVE: 2022-1660	This strike exploits an insecure deserialization vulnerability in Keysight N6854A and N6841A RF Sensor. The vulnerability is due to blind deserialization of untrusted data without any validation. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted HTTP request with malicious serialized data. Successful exploitation would result in arbitrary code execution with SYSTEM privileges. *NOTE: In one-arm mode, the strike executes the notepad binary on the target system whose process can be viewed from Task Manager
Strike KeySight N6854A and N6841A RF Sensor UserFirmwareRequestHandler Directory Traversal	CWE: 23 CVE: 2022-1661	This strike exploits a directory traversal vulnerability exists in KeySight N6854A and N6841A RF Sensor Software. This vulnerability is due to incomplete input sanitization in Java class UserFirmwareRequestHandler. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted request. Successful exploitation could read arbitrary files on the target server under the security context of the SYSTEM.
Strike Oracle JDeveloper ADF Faces Deserialization of Untrusted Data Vulnerability	CVE: 2022-21445 CWE: 502	This strike exploits an insecure deserialization vulnerability in Oracle JDeveloper ADF Faces. The vulnerability is due to insufficient validation of HTTP request. A remote unauthenticated attacker can exploit this vulnerability by sending crafted HTTP request to the vulnerable server. Successful exploitation of this vulnerability could lead to remote code execution in the context of the user using the vulnerable server.
Strike Gitlab Project Import Remote Code Execution	CWE: 732 CVE: 2022-2185	This strike exploits an OS command injection vulnerability in Gitlab. The vulnerability is due to improper handling of the import_source field. A remote Authenticated attacker can exploit the vulnerability by performing a bulk import from a server controlled by the attacker. Successful exploitation can result in remote code execution. Note: This strike includes just the last part of the attack where targeted server requires data from the custom server controlled by the attacker and the attacker's response.
Strike Apache httpd mod_lua req_parsebody Denial of Service	CWE: 665 CVE: 2022-22719	This strike exploits a denial of service vulnerability in Apache httpd. The vulnerability is due to use of uninitialized memory when processing a request. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could lead to crash of the server and with extended exploitation may lead to denial of service conditions.
Strike VMware Spring Cloud Gateway SpEL Code Injection	CWE: 94 CVE: 2022-22947	This strike exploits a remote code execution vulnerability in Spring Cloud Gateway. The vulnerability is due to improper validation of user-provided SpEL expressions. A remote attacker could exploit this vulnerability by sending a maliciously crafted request to an application using a vulnerable version of Spring Cloud Gateway. Successful exploitation could lead to remote code execution. *NOTE: When running this strike in OneArm mode, the strike will attempt to create a file called poc.txt in /tmp folder.

Name	References	Description
Strike Vmware Workspace ONE Access Freemarker Server-side Template Injection	CWE: 94 CVE: 2022-22954	This strike exploits a server side template injection vulnerability in VMware Workspace ONE Access and Identity Manager. The vulnerability is due to server-side template injection in the deviceUdid parameter. A remote, unauthenticated attacker can exploit this vulnerability by sending crafted requests. Successful attack can result in remote code execution on the target server.
Strike Spring Expression Resource Access Vulnerability	CWE: 94 CVE: 2022-22963	This strike exploits a remote code execution vulnerability in Spring Cloud Foundation. The vulnerability is due to lack of validation of the values provided in spring.cloud.function.routing-expression header in the HTTP packet. A remote unauthenticated attacker could exploit this vulnerability by embedding a specially crafted Spring Expression Language(SpEL) as a routing-expression in the HTTP packet which could lead to Remote Code Execution on the server. *NOTE: In one-arm, the strike will attempt to create a file named PWNED in the /tmp directory.
Strike VMware Spring Framework Data Binding ClassLoader	CWE: 94 CVE: 2022-22965	This strike exploits a remote code execution vulnerability in Spring Cloud Foundation. The vulnerability is due to inadequate validation of parameters used for data binding, allowing for manipulation of the ClassLoader. A remote attacker could exploit this vulnerability by providing a crafted parameter in an HTTP request. Successful exploitation could lead to ClassLoader manipulation, which may lead to execution of arbitrary code under the security context of the container of the target application. *NOTE: In one-arm, the strike will attempt to create a webshell at webapps/ROOT/shell.jsp which can be used for Remote Code Execution.
Strike SalesAgility SuiteCRM email_recipients Remote Code Execution Vulnerability	CVE: 2022-23940	This strike exploits a remote code execution vulnerability in SalesAgility SuiteCRM. The vulnerability is located in the improper input validation of the "email_recipients" parameter within HTTP POST requests. Exploiting this vulnerability allows a remote, authenticated attacker to execute arbitrary code on the target server.
Strike Apache APISIX batch-requests Plugin IP address Restriction Bypass	CWE: 290 CVE: 2022-24112	This strike exploits an authentication weakness vulnerability in Apache APISIX. The vulnerability is due to inefficient validation of client requests at the vulnerable API endpoint "/apisix/admin/batch-requests". A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the vulnerable server if the batch-requests plugin is enabled and it is using the default API key of the administrator. Successful exploitation could lead to arbitrary code execution under the security context of the server process. *NOTE: While running this strike in OneArm mode, it creates a new endpoint/route "/poc/testing" which is visited to execute a command to create a file called "poc" under the "/tmp" directory on the server.
Strike Apache Airflow DAG OS Command Injection	CWE: 78 CVE: 2022-24288	This strike exploits a command injection vulnerability in Apache Airflow. This vulnerability is due to improper input validation for parameters "foo" and "miff" for directed acyclic graphs or DAGs. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successfully exploiting this vulnerability could result in command execution in the context of the user running the server. *NOTE : In one-arm mode, the strike uses airflow/airflow to login and uses example_passing_params_via_test_command DAG for exploitation which results in /tmp/test file being created.

Name	References	Description
Strike Zimbra Webmail Cross-Site Scripting	CVE: 2022-24682 CWE: 79	This strike exploits reflected cross-site scripting vulnerability in Zimbra Collaboration server. This vulnerability is due to insufficient input validation in the Calendar feature. A remote attacker could exploit this vulnerability by enticing the target to click on a crafted link. Successful exploitation could result in execution of script code in the security context of the target user's browser.
Strike MyBB Admin Control Panel Code Injection Vulnerability	CVE: 2022-24734	This strike targets a code injection vulnerability in the MyBB Admin Control Panel. The issue arises from improper input validation when processing user-supplied data in the settings management functionality. Exploiting this vulnerability allows a remote, authenticated attacker to execute arbitrary PHP code on the server with the privileges of the web application.
Strike Google Chrome ServiceWorkerVersion Use After Free	CWE: 416 CVE: 2022-2480 GOOGLE: 2321	This strike exploits a type confusion vulnerability in Google Chrome. Specifically, when the ServiceWorkerVersion::MaybeTimeoutRequest method is called it will remove the last reference to the version object which is bound to the callback and will cause the object's destruction. If this happens the MaybeTimeoutRequest function will attempt to access the freed object by means of its <code>inflight_requests_</code> field. When this happens a denial of service condition, or potentially remote code execution, may occur in the context of the browser process.
Strike TerraMaster TOS Unauthenticated Remote Code Execution	CWE: 74 CVE: 2022-24989	This strike exploits an unauthenticated command injection vulnerability in TerraMaster TOS. The vulnerability is due to the improper sanitization of the user input used in the <code>popen</code> function of the <code>createRaid</code> function. The vulnerability when chained with CVE-2022-24990 allows a remote unauthenticated attacker to execute arbitrary code as root through the <code>raidtype</code> and <code>diskstring</code> parameters during PHP Object Instantiation at the <code>api.php?mobile/createRaid</code> endpoint. Successful exploitation could result in arbitrary code execution under the security context of the user running the vulnerable application with root privileges.
Strike TerraMaster TOS Sensitive Information Leak Vulnerability	CWE: 306 CVE: 2022-24990	This strike exploits a sensitive information leak vulnerability in TerraMaster TOS. The vulnerability arises due to <code>webNasIPS</code> function in TerraMaster NAS devices which skips authentication checks. Attackers can exploit this vulnerability to obtain sensitive information like the admin password hash without authentication. The vulnerability when chained with CVE-2022-24989 allows a remote unauthenticated attacker to execute arbitrary code as root. Successful exploitation could result in information disclosure and in the worst case it could lead to remote code execution under the security context of the target server.
Strike Delta Industrial Automation DIAEnergie Arbitrary File Upload Vulnerability cve_2022_25347	CVE: 2022-25347	This strike exploits an arbitrary file upload vulnerability in Delta Industrial Automation DIAEnergie. The vulnerability resides in the <code>HandlerPage_KID</code> endpoint, where insufficient input validation is performed on the <code>HtmlId</code> parameter and file extensions during file upload processing. A remote, unauthenticated attacker could leverage this flaw to upload malicious files to arbitrary locations on the server, potentially leading to the execution of arbitrary code within the web server's context.

Name	References	Description
Strike Atlassian Confluence OGNL Injection	CWE: 74 CVE: 2022-26134	This strike exploits an OGNL injection vulnerability in the Confluence Server and Data Center. The vulnerability is due to improper validation of the URL of a HTTP request. A successful attack can result in arbitrary command execution in the context of the server process.
Strike Atlassian Confluence App Hard-coded Credentials Vulnerability	CWE: 798 CVE: 2022-26138	The strike exploits a use of hardcoded credentials vulnerability in the web component of the Atlassian Confluence app. The vulnerability is due to the use of hardcoded credentials, specifically the username disabledsystemuser and the password disabled1system1user6708. A remote, unauthenticated attacker with knowledge of these default credentials could log into Confluence and access all content available to users in the confluence-users group. Successful exploitation could result in information disclosure.
Strike Open-Falcon Falcon-Plus SQL Injection in GetHostsFromGroup Function	CVE: 2022-26245	This strike exploits a SQL injection vulnerability in Open-Falcon Falcon-Plus. The vulnerability exists due to improper sanitization of user input in the /proc/group API endpoint. A remote attacker could leverage this flaw by sending a specially crafted request, leading to arbitrary SQL query execution on the database.
Strike Watchguard Fireware buffer overflow	CWE: 119 CVE: 2022-26318	This strike exploits a buffer overflow vulnerability in Watchguard Fireware. The vulnerability is due to improper validation of user input. A remote, unauthenticated attacker could exploit this vulnerability by submitting a specially crafted HTTP request which could result in arbitrary command execution in the context of NOBODY user. Note: In one-arm, a reverse shell is executed to the IP 192.168.102.113, port 8888.
Strike dotCMS processFile Directory Traversal	CWE: 22 CVE: 2022-26352	This strike exploits a Directory Traversal vulnerability in dotCMS. The vulnerability is due to insufficient validation of the names of files uploaded through the dotCMS content API. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in writing a file outside of the expected document root, possibly leading to, in the worst case, arbitrary code execution under the security context of the web server process. *NOTE: While running this strike in OneArm mode, a file named "poc.jsp" is created on the server.
Strike Delta Industrial Automation DIAEnergie SQL Injection Vulnerability in DIAE_loopmapHandler.ashx	CVE: 2022-26887	This strike exploits an SQL injection vulnerability in Delta Industrial Automation DIAEnergie. The vulnerability resides in the insufficient input validation of the "kid" parameter in HTTP requests to the DIAE_loopmapHandler.ashx endpoint. A remote, unauthenticated attacker could exploit this vulnerability by sending specially crafted requests, leading to the execution of arbitrary SQL commands with the privileges of NT SERVICE\MSSQLSERVER.
Strike Studio-42 elFinder Unrestricted File Upload Vulnerability	CVE: 2022-27115	This strike exploits an unrestricted file upload vulnerability in Studio-42 elFinder. The vulnerability resides in the improper validation of filenames during file uploads via the connector.minimal.php endpoint on Windows systems. Exploiting this vulnerability allows a remote, unauthenticated attacker to upload files with restricted extensions or malicious content, potentially leading to remote code execution.

Name	References	Description
Strike QNAP Photo Station Externally Controlled Reference Vulnerability	CWE: 610 CVE: 2022-27593	This strike exploits an externally controlled reference to a resource vulnerability in QNAP NAS devices running Photo Station. The vulnerability arises from an anomaly in PHP's fopen function, enabling an attacker to manipulate the 'g' parameter to traverse outside the intended cache directory and write cached files to arbitrary locations. Successful exploitation of this vulnerability would enable an attacker to modify system files. A remote, unauthenticated attacker could potentially fill up storage areas or exhaust other critical resources on the NAS, leading to denial of service for legitimate users or services dependent on those resources.
Strike Zoho ManageEngine OpManager SQL Injection in Inventory Reports	CVE: 2022-27908	This strike exploits a SQL injection vulnerability in Zoho ManageEngine OpManager. The vulnerability resides in the Inventory Reports module due to insufficient validation of HTTP request parameters. A remote, authenticated attacker could leverage this flaw to execute arbitrary SQL queries, potentially compromising the underlying database.
Strike Zimbra Collaboration Memcached CRLF Injection	CVE: 2022-27924 CWE: 93	This strike exploits a CRLF(Carriage Return followed by Line Feed) Injection vulnerability in the Zimbra Collaboration server. This vulnerability is due to insufficient sanitization of CRLF characters in HTTP Request-URIs and HTTP header values when performing route caching using Memcached. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could allow an attacker to inject arbitrary Memcached commands which would be executed by the server.
Strike Zimbra Collaboration MailboxImportServlet Authenticated Directory Traversal	CWE: 22 CVE: 2022-27925	This strike exploits an authenticated directory traversal vulnerability in Zimbra Collaboration. The vulnerability is due to improper validation of zip files uploaded to the MailboxImportServlet. A remote, authenticated attacker could exploit this vulnerability by uploading a crafted zip file to the target server. Successful exploitation could result in the attacker writing files outside of the expected document root, in the worst case, leading to arbitrary code execution under the security context of the server process.
Strike Zoho ManageEngine ADSelfService Plus Custom Script Command Injection	CWE: 78 CVE: 2022-28810	This strike exploits a command injection vulnerability in Zoho ManageEngine ADSelfService Plus. This vulnerability is due to insufficient sanitization of password field in the policy custom script. The attacker authenticates as the admin user in the vulnerable application and then sends a crafted HTTP POST request to the vulnerable server with malicious parameters which are the JSON values SCRIPT_COMMAND_RESET and SCRIPT_COMMAND_UNLOCK within the APC_SETTINGS_DETAILS. The vulnerability is triggered when a user changes or resets their password, or unlocks their account through ADSelfService Plus. Successful exploitation could result in command injection. *Note : Upon running the strike in one-arm mode, the output of command 'whoami' is appended to C:\ProgramData\randomfile.txt each time a victim changes or resets their password, or unlocks their account. The default credentials being used are admin/admin.

Name	References	Description
Strike SolarView Compact Command Injection	CWE: 78 CVE: 2022-29303	This strike exploits a command injection vulnerability in SolarView Compact. This vulnerability lies in the conf_mail.php component of the SolarView application. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted post request to the target server. Successful exploitation of this vulnerability could lead to remote code execution.
Strike WSO2 API Manager Directory Traversal	CWE: 434 CVE: 2022-29464	This strike exploits a directory traversal vulnerability in WSO2 API Manager. The vulnerability is due to improper sanitization for the multipart form field name for the file upload route. A remote, unauthenticated attacker could exploit the vulnerability by sending crafted HTTP requests to a target server. Successful exploitation can result in arbitrary file write in the context of the wso2carbon user.
Strike Mitel MiVoice Connect Data Validation Vulnerability	CWE: 20 CVE: 2022-29499	This strike exploits a server-side request forgery vulnerability in Mitel MiVoice. The vulnerability arises due to improper input validation of the get_url parameter in the vtest.php script. A remote, unauthenticated attacker can exploit this flaw to force the application to make an internal request to ucbsync.php, which is normally inaccessible from external sources. Successful exploitation can lead to remote code execution.
Strike Lansweeper HelpdeskActions.aspx Directory Traversal Vulnerability	CVE: 2022-29517	This strike exploits a directory traversal vulnerability in Lansweeper. The vulnerability exists due to insufficient sanitization of the inline attachment file names when editing templates. A remote, authenticated attacker could leverage this flaw to write arbitrary files to the target system, potentially leading to denial of service or other malicious outcomes.
Strike Microsoft Windows Support Diagnostic Tool (MSDT) Follina RCE	CWE: 829 CVE: 2022-30190	This strike exploits an remote code execution vulnerability AKA Follina in Microsoft Support Diagnostic Tool(MSDT) when MSDT is called using the URL protocol. The vulnerability is due to the MSDT tool executing arbitrary code. A remote unauthenticated attacker can trick the victim into downloading a malicious HTML file served by the attacker which might execute arbitrary code on the victim machine. *NOTE: The link to the malicious file can be embedded in a Word Document which can download the HTML file without any interaction. This vulnerability can also be exploited by invoking any web request command in Powershell. The strike simulates the latter scenario where the client downloads the malicious HTML from the server.
Strike Google Chrome NotifyCompleted Use After Free	CWE: 416 CVE: 2022-3038 GOOGLE: 2324	This strike exploits a vulnerability in Google Chrome. Specifically, when SetUpUpload posts a task with a bound raw loader pointer using the default task runner, it's possible for the loader to get destroyed before the task is executed, resulting in NotifyCompleted accessing freed memory. When this happens a denial of service condition, or potentially remote code execution, may occur.

Name	References	Description
Strike Zyxel Firewall CGI Command Injection	CWE: 78 CVE: 2022-30525	This strike exploits a command injection vulnerability in Zyxel Firewall. The vulnerability is due to improper input validation in the CGI component. A remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the CGI component. A successful attack may result in remote code execution in the security context of nobody user.
Strike WWBN AVideo unzipDirectory Directory Traversal Vulnerability	CVE: 2022-30547	This strike exploits a directory traversal vulnerability in WWBN AVideo. The vulnerability resides in the unzipDirectory function within the objects/functions.php file, which fails to properly sanitize file names during ZIP file extraction. A remote, authenticated attacker could leverage this flaw by uploading a crafted ZIP file, enabling arbitrary file writes and potential code execution within the web server's security context.
Strike Lansweeper AssetActions.aspx Directory Traversal Vulnerability	CVE: 2022-32573	This strike exploits a directory traversal vulnerability in Lansweeper. The vulnerability exists due to improper sanitization of the "txtdocname" parameter when processing file uploads. Exploiting this flaw allows a remote, authenticated attacker to perform arbitrary file writes on the target system, potentially leading to denial of service or other malicious outcomes.
Strike Apache Spark Command Injection	CWE: 77 CVE: 2022-33891	This strike exploits a command injection vulnerability in Apache Spark. The vulnerability is due to improper validation of user input. A remote, unauthenticated attacker could exploit this vulnerability by submitting a specially crafted HTTP request which could result in arbitrary command execution in the context of the user running the server.
Strike Django Trunc and Extract SQL Injection	CVE: 2022-34265 CWE: 89	This strike exploits two SQL injection vulnerabilities in Django. The vulnerabilities are due to insufficient sanitization of user input to kind and lookup_name parameters passed to database functions Trunc and Extract respectively. A remote attacker can exploit the vulnerabilities by sending a crafted request to the target server. Successful exploitation could result in execution of arbitrary SQL statements. *NOTE: When running this strike in OneArm mode, it sends a malicious request to the target Django webapp, and creates a new table in the database.
Strike Zoho ManageEngine Password Manager Pro XMLRPC Insecure Deserialization	CVE: 2022-35405 CWE: 502	This strike exploits a remote code execution vulnerability in Zoho ManageEngine Password Manager Pro. The vulnerability is due to deserialization of untrusted data by the XMLRPC component. A remote attacker can exploit this vulnerability by sending crafted HTTP requests to the target server. Successful exploitation results in remote code execution.
Strike ZK Framework Authentication Bypass	CWE: 200 CVE: 2022-36537	This strike exploits an authentication bypass vulnerability in ZK Java Framework. The vulnerability is due to lack of authentication in ZK AuUploader servlet. A remote unauthenticated attacker can exploit this vulnerability by sending a crafted request to the victim server which leads to the disclosure of sensitive files in the context of the webroot.

Name	References	Description
Strike Atlassian Bitbucket Server and Data Center Command Injection	CWE: 78 CVE: 2022-36804	This strike exploits a command injection vulnerability in Atlassian Bitbucket Server and Data Center. The vulnerability is due to improper validation of certain user input fields. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target repository to request an archive which injects an argument to run an OS command. Successful exploitation of the vulnerability could lead to arbitrary command execution under the security context of the service. *NOTE: While running this strike in OneArm mode, a file /tmp/poc is created on the server.
Strike Zimbra Collaboration MailboxImportServlet Authentication Bypass	CWE: 22 CVE: 2022-37042	This strike exploits an authentication bypass vulnerability in Zimbra Collaboration. The vulnerability is due to improper validation of zip files uploaded to the MailboxImportServlet. A remote, unauthenticated attacker could exploit this vulnerability by uploading a crafted zip file to the target server. Successful exploitation could result in the attacker writing files outside of the expected document root, in the worst case, leading to arbitrary code execution under the security context of the server process.
Strike Adobe ColdFusion Directory Traversal and Arbitrary Code Execution Vulnerability	CVE: 2022-38421	This strike exploits a directory traversal vulnerability in Adobe ColdFusion. The vulnerability exists due to improper input validation when processing HTTP parameters in the copydirectory.cfm script. A remote, authenticated attacker could leverage this flaw to execute arbitrary code with SYSTEM privileges on the target server.
Strike Google Chrome SetChangePassword ResponseCode Use After Free	CWE: 416 CVE: 2022-3842 GOOGLE: 2348	This strike exploits a vulnerability in Google Chrome. Specifically, a vulnerability exists inside WellKnownChangePasswordState::SetChangePasswordResponseCode function. It is possible to craft javascript in such a way that a Use After Free condition can trigger. When this happens a denial of service condition, or potentially remote code execution, may occur.
Strike Apache Airflow DAG run_id Command Injection	CWE: 94 CVE: 2022-40127	This strike exploits a command injection vulnerability in Apache Airflow. This vulnerability is due to improper input validation for parameter run_id for directed acyclic graphs or DAGs. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successfully exploiting this vulnerability could result in command execution in the context of the user running the server. *NOTE : In one-arm mode, the strike uses airflow/ airflow to login and uses example_bash_operator DAG for exploitation which results in /tmp/Test file being created.
Strike pfSense pfBlockerNG Host Header Command Injection	CWE: 78 CVE: 2022-40624	This strike exploits a command injection vulnerability in Netgate pfSense pfBlockerNG. This vulnerability is due to improper input validation for the Host HTTP header. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successfully exploiting this vulnerability could result in OS command injection in the context of root.

Name	References	Description
Strike Fortinet Multiple Products Administrative Interface Authentication Bypass	CWE: 288 CVE: 2022-40684	This strike exploits an Authentication Bypass vulnerability in multiple Fortinet products, including FortiOS, FortiProxy, and FortiSwitchManager. The vulnerability is due to errors in handling certain HTTP headers in user requests. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in an attacker bypassing authentication and executing commands as an admin user on the target system.
Strike Dolibarr ERP and CRM Code Injection Vulnerability in edit.php	CVE: 2022-40871	This strike exploits a code injection vulnerability in Dolibarr ERP and CRM. The vulnerability resides in the insufficient sanitization of parameters in HTTP POST requests to the edit.php endpoint. Successful exploitation allows a remote attacker to execute arbitrary PHP code on the target server, potentially leading to remote code execution.
Strike Microsoft Exchange Server Server-Side Request Forgery Vulnerability	CWE: 918 CVE: 2022-41040	This strike exploits a server-side request forgery vulnerability in Microsoft Exchange Server. The vulnerability is due to insufficient handling of requests to the autodiscover component of Exchange. An authenticated, remote attacker can exploit this vulnerability by sending a crafted request to the vulnerable Exchange server. Successful exploitation results in requests being made to backend servers. *NOTE: This strike sends a request to /mapi/nsipi/ or ews/exchange.asmx which are inaccessible by default. In one-arm mode we use the authorization Administrator:Password1
Strike Centreon Web Poller Resource SQL Injection Vulnerability	CVE: 2022-41142	This strike exploits a SQL injection vulnerability in the Centreon Web Poller Resource module. The vulnerability exists due to insufficient input validation of the `resource_activate[resource_activate]` parameter in the `insertResource` function. A remote, authenticated attacker could leverage this flaw by sending a specially crafted HTTP request, potentially leading to arbitrary SQL command execution on the target database.
Strike pgAdmin validate_binary_path Remote Code Execution	CWE: 78 CVE: 2022-4223	This strike exploits a remote code injection vulnerability in pgAdmin. The vulnerability is due to insufficient input validation of the utility_path parameter sent to the validate_binary_path endpoint. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted request to the vulnerable endpoint. Successful exploitation would result in execution of arbitrary code in the security context of the service. *NOTE: While running this strike in OneArm mode, a file /tmp/poc is created on the server.
Strike Centreon Web formContactGroup.php SQL Injection Vulnerability	CVE: 2022-42427	This strike exploits an SQL injection vulnerability in the Centreon Web application. The vulnerability exists due to improper validation of the `cg_id` parameter in the `formContactGroup.php` script. A remote, authenticated attacker could leverage this flaw by sending a specially crafted HTTP request, potentially leading to the execution of arbitrary SQL commands on the database.

Name	References	Description
Strike Apache Common Text Library Text4Shell RCE	CWE: 94 CVE: 2022-42889	This strike exploits a Remote code execution vulnerability in Apache Commons Text. This vulnerability is due to insecure string interpolation defaults. A remote attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in the execution of arbitrary code. *NOTE: In one-arm mode, the strike either creates a random file in the /tmp folder of the server or makes the server reach out to a malicious attacker controlled host at ip - 10.39.44.149 and port - 8080.
Strike Zoho ManageEngine Password Manager Pro UserGroupListTable Controller SQL Injection	CWE: 89 CVE: 2022-43672	The strike exploits an SQL injection vulnerability in Zoho ManageEngine Password Manager Pro and related products. The vulnerability is due to improper validation of actionType parameter in the UserGroupListTableController class. A remote attacker can exploit the vulnerability by sending a crafted request to the target server. Successful exploitation could lead to arbitrary SQL code execution in the security context of database service, which runs as SYSTEM.
Strike Atlassian Bitbucket Server and Data Center Command Injection Vulnerability	CWE: 77 CVE: 2022-43781	This strike exploits a command injection vulnerability in Atlassian Bitbucket Server and Data Center. The vulnerability is due to improper validation of usernames on the server. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in arbitrary command execution in the security context of the user running the vulnerable application. *NOTE: While running this strike in OneArm mode, a file /tmp/poc is created on the server.
Strike Contec CONPROSYS HMI System chkFormula Command Injection	CVE: 2022-44456 CWE: 78	This strike exploits a vulnerability in the Contec CONPROSYS HMI system. A vulnerability exists due to insufficient sanitation when parsing JSON object and will be triggered when the attacker parses the JSON object with the injected escape character, which allows remote code execution to occur in the context of the web server.
Strike TP-Link Archer AX21 Country Command Injection	CVE: 2023-1389 CWE: 77	This strike exploits a command injection vulnerability in TP-Link Archer AX21. The vulnerability is due to the improper sanitization of the country parameter. A remote, unauthenticated attacker could exploit this vulnerability by injecting the commands into the country parameter. Execution requires sending the request twice, the first request sets the command in the country value, and the second request executes it. Successful exploitation could allow an attacker to achieve remote code execution with root privileges.
Strike Sophos Web Appliance Command Injection Vulnerability	CWE: 77 CVE: 2023-1671	This strike exploits a pre-auth command injection vulnerability in the warn-proceed handler of the Sophos Web Appliance. The vulnerability arises due to improper sanitization of user-provided input. It allows a remote, unauthenticated attacker to inject commands through the data field by escaping commands with a single quote. Successful exploitation could result in arbitrary code execution under the security context of the user running the vulnerable application.

Name	References	Description
Strike WordPress Limit Login Attempts Plugin Stored Cross Site Scripting	CWE: 79 CVE: 2023-1861	A stored cross-site scripting vulnerability has been discovered in WordPress Limit Login Attempts Plugin. The vulnerability is due to improper input validation of the cookie value. A remote, unauthenticated attacker could exploit this vulnerability by sending requests with crafted cookie to the target system. Successful exploitation could result in stored cross-site scripting. The vendor has released a patch to address this vulnerability in plugin version 1.7.2.
Strike Cisco IOS XE WebUI Authentication Bypass	CWE: 284 CVE: 2023-20198	This strike exploits an authentication bypass vulnerability in the WebUI component of Cisco IOS XE. This vulnerability is due to improper configuration of the nginx reverse proxy server. A remote, unauthenticated attacker can exploit this vulnerability to bypass authentication by accessing an internal endpoint. Successful exploitation results in the ability to issue privilege commands, including to create a new local user.
Strike Cisco IOS XE WebUI Command Injection	CWE: 78 CVE: 2023-20273	This strike exploits a command injection vulnerability in the WebUI component of Cisco IOS XE. This vulnerability is due to insufficient validation of IPv6 addresses supplied when performing a software upgrade. A remote, authenticated attacker can exploit this vulnerability by sending crafted HTTP requests to the target server. Successful exploitation results in the execution of arbitrary OS commands with the privileges of root.
Strike VMware Aria Operations for Logs InternalClusterController Insecure Deserialization	CWE: 502 CVE: 2023-20864	An insecure deserialization vulnerability has been reported in VMware Aria Operations for Logs. The vulnerability is due to improper validation of user data. A remote unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in arbitrary code execution under the security context of the root user.
Strike Vmware Aria Operations for Networks resttosaasservlet Command Injection Vulnerability	CWE: 77 CVE: 2023-20887	This strike exploits a command injection vulnerability in Vmware Aria Operations for Networks. The vulnerability is due to improper input handling in API requests and an Nginx misconfiguration that allows access to the restricted internal API endpoint /resttosaasservlet. A remote, unauthenticated attacker can exploit this vulnerability by sending specially crafted requests, bypassing the Nginx reverse proxy configuration. Successful exploitation can lead to the execution of arbitrary commands on the underlying operating system with root privileges, potentially resulting in full system compromise.
Strike VMware Aria Operations for Networks saveFileToDisk Directory Traversal Vulnerability	CWE: 22 CVE: 2023-20890	This strike exploits a directory traversal vulnerability in VMware Aria Operations for Networks. The vulnerability is due to improper validation of file names when uploading files to the appliance. The filename parameter from the multipart request is not sanitized before it is used to create a path to the file. A remote, authenticated attacker could exploit this vulnerability by sending crafted requests to the target server. Successful exploitation will allow an attacker to write files outside of the expected temp directories. In the worst case, this could be leveraged to achieve arbitrary code execution under the security context of the root user.

Name	References	Description
Strike Wordpress WpForo Plugin LFI SSRF Deserialization	CWE: 98 CVE: 2023-2249	This strike exploits a File Inclusion and Server Side Request Forgery (SSRF) vulnerability in wpforo plugin of wordpress. This vulnerability is due to lack of input validation for the image_blob parameter which is passed to the php get_file_contents method call. A remote, authenticated low-privileged attacker could exploit this vulnerability by sending a crafted request to the target wordpress server. A successful attack may result in local file inclusion, server side request forgery or insecure deserialization in the server. *NOTE: In one-arm, the strike attempts to login with the creds - 'victimtest/1234' and attempts to fetch the contents of /etc/passwd or reach an internal endpoint at 'http://10.39.44.149:4445/secret' depending on the variant being ran.
Strike Atlassian Confluence Data Center and Server Setup Action Privilege Escalation	CWE: 863 CVE: 2023-22515	This strike exploits a privilege escalation vulnerability in Atlassian Confluence Data Center and Server. The vulnerability is attributed to a weakness in access control within the setup actions component. Its root cause lies in the attacker's ability to execute complex getter/setter chains on the Action object for unauthenticated endpoints, allowing manipulation of crucial properties. Through the modification of the setupComplete variable, the attacker successfully exploited the setup functionality, resulting in the creation of a new administrator user. An unauthenticated, remote attacker could leverage this vulnerability by sending meticulously crafted requests to the setup endpoint. Successful exploitation could lead to the execution of arbitrary code within the security context of the newly created administrator user.
Strike Atlassian Confluence Data Center and Server Improper Authorization	CWE: 863 CVE: 2023-22518	This strike exploits an improper authorization vulnerability in Atlassian Confluence Data Center and Server. The vulnerability arises from the absence of authentication for legacy endpoints associated with the application restore feature, specifically the "/json/setup-restore.action" endpoint. Given the lack of authentication requirements for accessing this endpoint, a malicious actor could exploit this vulnerability to delete all data in a Confluence installation and replace it with data under their control. A remote, unauthenticated attacker could leverage this vulnerability by sending carefully crafted requests to the target server. If successfully exploited, this could lead to privilege escalation and the potential execution of arbitrary code on the targeted system.
Strike Atlassian Confluence Data Center and Server Template Injection	CWE: 74 CVE: 2023-22527	This strike exploits a template injection vulnerability in Atlassian Confluence Data Center and Server. The vulnerability is due to improper validation of user data sent to the sever. The label parameter is not properly escaped before use in an OGNL expression. This allows arbitrary OGNL expression evaluation. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted requests to the target server. Successful exploitation could result in arbitrary code execution under the security context of the user running the vulnerable application. *NOTE: While running the strike in one-arm mode, a file gets created in the /tmp directory of the vulnerable server.

Name	References	Description
Strike Zoho ManageEngine SupportCenter Plus Command Injection via Custom Schedules Executor	CVE: 2023-23076	This strike exploits a command injection vulnerability in Zoho ManageEngine SupportCenter Plus. The vulnerability exists due to insufficient validation of the "executor" parameter in the custom schedule settings. A remote, authenticated attacker could leverage this flaw by sending specially crafted requests, leading to arbitrary command execution with SYSTEM privileges.
Strike Joomla CMS Webservice Authentication Bypass	CWE: 284 CVE: 2023-23752	This strike exploits an authentication bypass vulnerability in Joomla CMS. The vulnerability is due to inadequate sanitization of request parameters when processing API requests. If the request includes a 'public' parameter its value will overwrite the route default variable, and unauthenticated access may be granted to private API routes. An unauthenticated remote attacker can manipulate request parameters, leading to potential unauthorized access to private API routes that require authentication. Successful exploitation could result in sensitive information disclosure, including Joomla database credentials. Attackers could leverage this information to gain unauthorized access, modify user passwords, or perform brute-force attacks on user accounts. *Note: Running this strike in one-arm mode reveals the database credentials and other sensitive information.
Strike Citrix ShareFile Storage Zones Controller ProcessRawPostedFile Directory Traversal	CWE: 284 CVE: 2023-24489	This strike exploits a directory traversal vulnerability in the Upload module of the Citrix ShareFile Storage Zones Controller. The vulnerability is due to improper validation of user input in the ProcessRawPostedFile function. A remote, unauthenticated attacker could exploit this vulnerability by sending a request with a crafted uploadId request parameter to the target server. Successful exploitation could allow an attacker to save files to an arbitrary file path under the web root directory, which could lead to the execution of arbitrary code.
Strike D-Link DIR-820 Router ping.ccp OS Command Injection	CVE: 2023-25280 CWE: 78	This strike exploits an OS command injection vulnerability in D-Link DIR-820 Router. The vulnerability is due to improper sanitization of ping_addr parameter used in ping.ccp endpoint. A remote, unauthenticated attacker can exploit this vulnerability by sending a crafted payload to the ping_addr parameter. Successful exploitation could result in remote code execution on the affected device and potential escalation of privileges to root.
Strike Ruckus Wireless Admin Unauthenticated RCE	CWE: 94 CVE: 2023-25717	This strike exploits a remote code execution vulnerability in Ruckus Wireless routers. The vulnerability is due to insufficient input validation in the '/forms/doLogin' endpoint of the admin web page. A remote unauthenticated attacker can exploit this vulnerability by sending crafted requests to the victim router which results in remote code execution.
Strike Adobe ColdFusion convertToTemplateProxy Insecure Deserialization	CWE: 502 CVE: 2023-26360	This strike exploits an insecure deserialization vulnerability in Adobe ColdFusion. The vulnerability is due to deserialization of untrusted data when processing HTTP parameters sent to ColdFusion Component (CFC) endpoints. A remote, unauthenticated, attacker could exploit this vulnerability by injecting crafted CFML tags into logs and then trigger the exploit by requesting the log file. Successful exploitation could result in arbitrary code execution in the security context of SYSTEM.

Name	References	Description
Strike PaperCut MF and NG SetupCompleted formSubmit Authentication Bypass	CVE: 2023-27350 CWE: 284	This strike exploits an authentication bypass vulnerability in PaperCut MF/NG. The vulnerability is due to improper access and authentication control in "SetupCompleted" class. A remote, unauthenticated attacker could exploit the vulnerability by sending a request to the "/app" endpoint on the target server. Successful exploitation could result in authentication bypass and, in the worst case, arbitrary code execution on the server under the security context of SYSTEM. *NOTE - While running this strike in OneArm mode, windows calculator application runs on the target server.
Strike Zoho ManageEngine ADSelfService Plus Mobile App Authentication API Denial of Service	CWE: 476 CVE: 2023-28342	This strike exploits an authentication bypass vulnerability in Zoho ManageEngine ADSelfService Plus. The vulnerability is due to improper input validation in the Mobile App Authentication API. A remote, unauthenticated attacker could send a crafted request to the authentication endpoint without a password parameter. When the target server processes the request, it will pass the null password value to a native function resulting in an access violation and subsequently terminating and restarting the server process. Successfull exploition could result in denial of service.
Strike Contec CONPROSYS HMI System SQL Injection Vulnerability	CVE: 2023-29154 CWE: 89	This strike exploits an SQL injection vulnerability in Contec CONPROSYS HMI System. The vulnerability is due to insufficient sanitization of user data used in query_getTableCol.php. The query retrieves the metadata of the database table. However, the code fails to check for SQL injection characters in the JSON parameter of the table. As a result, a remote, authenticated attacker could exploit this vulnerability by sending a specially crafted request to the target server. A successful attack may allow the execution of arbitrary SQL commands against the database on the target server.
Strike Ghost CMS static-theme.js Directory Traversal Vulnerability	CVE: 2023-32235	This strike exploits a directory traversal vulnerability in Ghost CMS. The vulnerability resides in the static-theme.js component, where user-supplied paths are improperly validated. A remote attacker could leverage this flaw to access sensitive files on the server, potentially exposing confidential information.
Strike Ignite Realtime Openfire Path Traversal Vulnerability	CWE: 22 CVE: 2023-32315	This strike exploits a path traversal vulnerability in Ignite Realtime Openfire. This vulnerability is due to the improper handling of UTF-16 encoded characters in URLs. It allows an unauthenticated user to use an already configured Openfire environment to access restricted pages in the Admin Console reserved for administrative users. This vulnerability can be used to create a new admin user, which can then be used to upload a Openfire management plugin weaponized with a Java native payload that triggers an RCE. Successful exploitation could result in authentication bypass and remote code execution through access to the restricted Admin Console pages. *NOTE: While running the strike in one-arm mode, the CSRF token can be retrieved from the response, which can be further used to create a new admin user account.

Name	References	Description
Strike Ivanti Avalanche Remote Control Server updateSkin Directory Traversal	CWE: 22 CVE: 2023-32563	This strike exploits a directory traversal vulnerability in Ivanti Avalanche Remote Control Server. The vulnerability is due to improper input validation of the updateSkin function. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in remote code execution in the context of SYSTEM.
Strike Jenkins Sidebar Link Plugin icon Directory Traversal Vulnerability	CVE: 2023-32985 CWE: 22	This strike exploits a directory traversal vulnerability in Jenkins Sidebar Link Plugin. This vulnerability is due to a directory traversal when handling link icons. The vulnerability exists when the function SidebarLinkPlugin.doCheckLinkIcon() is called, the value of the parameter value or the path that is created is never sanitized or normalized of directory traversal related characters. A remote, authenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successfully exploiting this vulnerability could result in information disclosure. *NOTE: While running this strike in OneArm mode, the existence of the file "/etc/passwd" on the target server is checked. The credentials used are as follows: the username is "jenkins_user" and the password is "jenkins".
Strike Zimbra Webmail Draftid Cross-Site Scripting	CWE: 79 CVE: 2023-34192	This strike exploits a cross-site scripting vulnerability in the web component of Zimbra Collaboration Suite. The vulnerability is due to improper input sanitization. A remote authenticated attacker could exploit this vulnerability by sending a crafted request to the target system. Successful exploitation could result in execution of script code in the security context of the target user's browser.
Strike Google Chrome V8 Engine JSStackCheck Type Confusion	CWE: 843 CVE: 2023-3420	This strike exploits a type confusion vulnerability in the V8 JavaScript engine of Google Chrome. The vulnerability is due to incorrect side effect modelling of JSStackCheck. A remote attacker could exploit this vulnerability by enticing a user into opening a crafted HTML page. Successful exploitation could result in execution of arbitrary code in the context of the Google Chrome sandbox.
Strike Progress MOVEit Transfer moveitisapi SQL Injection	CWE: 89 CVE: 2023-34362	This strike exploits an SQL injection vulnerability for MOVEit Transfer. This vulnerability is due to lack of input validation sent to the endpoints /MOVEitISAPI.dll and /guestaccess.aspx. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. A successful attack may result in arbitrary SQL command execution against the database on the target server.
Strike Progress MOVEit Transfer SILCertToUser SQL Injection	CWE: 89 CVE: 2023-35036	This strike exploits an SQL injection vulnerability in MOVEit Transfer. This vulnerability is due to insufficient input validation in the 'X-IPSGW-ClientCert' header of the request sent to the endpoint /certtousergw.aspx. A remote, unauthenticated attacker could exploit this vulnerability by injecting SQL injection payload in the issuer or the subject field of the certificate in the request. A successful attack may result in arbitrary SQL command execution against the database on the target server.

Name	References	Description
Strike Ivanti Endpoint Manager Mobile (EPMM) and MobileIron Core Authentication Bypass	CWE: 287 CVE: 2023-35082	This strike exploits an authentication bypass vulnerability in Ivanti Endpoint Manager Mobile. The vulnerability is due to a logic flaw and allows a remote unauthenticated attacker to access API endpoints on exposed management servers or resources without proper authentication. This access grants them the ability to execute various operations, potentially compromising sensitive information or modifying platform configurations.
Strike Progress MOVEit Transfer UserProcessPassChangeRequest SQL Injection	CWE: 89 CVE: 2023-36934	This strike exploits an SQL injection vulnerability in MOVEit Transfer. This vulnerability is due to insufficient validation of encrypted query parameters which is formed from the initial request sent to the /human.aspx of the server. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted requests to the target server. A successful attack would result in arbitrary SQL command execution against the database on the target server.
Strike Ivanti MobileIron Sentry uploadFileUsingFile Input Authentication Bypass Vulnerability	CWE: 863 CVE: 2023-38035	This strike exploits an authentication bypass vulnerability in MICS Admin Portal in Ivanti MobileIron Sentry. A remote, unauthenticated attacker can bypass authentication controls on the administrative interface due to an insufficiently restrictive Apache HTTPD configuration. Successful exploitation of this vulnerability could allow an attacker to bypass authentication and gain unauthorized access to the system.
Strike Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	CWE: 502 CVE: 2023-38203	This strike exploits an insecure deserialization vulnerability in Adobe ColdFusion. The vulnerability is due to inadequate filtering of Java class paths during the deserialization process, allowing remote, unauthenticated attackers to send maliciously crafted serialized objects. These objects can lead to arbitrary code execution within the application. ColdFusion uses a denylist to prevent certain classes from being deserialized, however, the class com.sun.rowset.JdbcRowSetImpl was not blocked, which attackers exploited. Successful exploitation of this vulnerability allows attackers to execute arbitrary code on the affected system.
Strike Adobe ColdFusion Insecure Deserialization	CWE: 502 CVE: 2023-38204	This strike exploits an insecure deserialization vulnerability in Adobe ColdFusion. The vulnerability is due to deserialization of untrusted data when processing HTTP parameters sent to ColdFusion Component (CFC) endpoints. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted requests to the target server. Specifically, an attacker can send an HTTP request to any valid CFC endpoint with the _cfclient parameter set to true and a crafted argumentCollection HTTP parameter, containing a WDDX packet with a struct element containing a type attribute set to a class name. Successful exploitation could result in arbitrary code execution in the security context of system.
Strike Adobe ColdFusion IPFilterUtils Improper Access Control CVE 2023-38205	CWE: 284 CVE: 2023-38205	This strike exploits an improper access control vulnerability in Adobe ColdFusion. The vulnerability is due to improper validation of the URL path by the IPFilterUtils class which was supposed to block access to sensitive endpoints if accessed from an IP address not from the allow list. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted requests with extra characters to the target server. Successful exploitation could result in access to the ColdFusion Administrator endpoints.

Name	References	Description
Strike Cacti Group graph_view.php SQL Injection Vulnerability	CWE: 89 CVE: 2023-39361	This strike exploits an SQL injection vulnerability in Cacti. The vulnerability is due to improper validation of user data in the graph_view.php script. The rfilter parameter is validated to be a valid regular expression, but not validated to prevent SQL injection. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted requests to the target server. Successful exploitation could result in arbitrary SQL command execution against the database on the target server. *NOTE - While running the strike in one-arm mode it creates a table named "POC" in the target server.
Strike Qlik Sense Path Traversal	CWE: 22 CVE: 2023-41266	This strike exploits a path traversal vulnerability in Qlik sense. A remote, unauthenticated attacker can exploit this by creating an anonymous session and sending maliciously crafted HTTP requests. Successful exploitation could allow the attacker to send further requests to unauthorized endpoints.
Strike Netgate pfSense Command Injection in GIF-GRE Interface Configuration	CVE: 2023-42326	This strike exploits a command injection vulnerability in Netgate pfSense. The vulnerability resides in the improper input validation of parameters in the interfaces_gif_edit.php and interfaces_gre_edit.php files. A remote, authenticated attacker could leverage this flaw by sending specially crafted HTTP POST requests, leading to the execution of arbitrary commands with root privileges.
Strike JetBrains TeamCity XML-RPC Authentication Bypass Vulnerability	CWE: 288 CVE: 2023-42793	This strike exploits an authentication bypass vulnerability in JetBrains TeamCity. The vulnerability is due to improper handling of requests using XML-RPC with the "/RPC2" suffix in the Request-URI, which bypasses authentication. Exploiting this vulnerability enables attackers to gain administrator-level access by sending crafted requests to the target server. With elevated privileges, attackers can execute arbitrary commands under the security context of the target server. *Note : While running the strike in one-arm mode, it creates a file /tmp/test on the target server.
Strike Nextgen Mirth Connect XStreamSerializer Insecure Deserialization Vulnerability	CWE: 502 CVE: 2023-43208	This strike exploits an insecure deserialization vulnerability in Nextgen Mirth Connect. This vulnerability is due to improper input validation of XML request body data. The vulnerability exploits the insecure usage of the Java XStream library to unmarshal XML payloads. This improper handling allows attackers to craft malicious XML payloads that can bypass security checks and execute code on the server. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successfully exploiting this vulnerability could result in remote code execution in the security context of SYSTEM. *NOTE : While running the strike as one-arm, the file /tmp/test gets created on the target server.
Strike Ivanti Avalanche FileStoreConfig Arbitrary FileUpload Vulnerability	CVE: 2023-46263 CWE: 434	This strike exploits an arbitrary file upload vulnerability in Ivanti Avalanche. The vulnerability is due to inadequate validation of the txtUncPath field in the Central FileStore configuration settings. A remote authenticated attacker can exploit this by setting the file storage path to target unauthorized directories, specifically the RemoteControl server's webroot. The insufficient checks allow the attacker to bypass blacklist restrictions, enabling malicious files to be uploaded and executed as SYSTEM on the server. Successful exploitation of this vulnerability could lead to remote code execution in the context of the user using the vulnerable server.

Name	References	Description
Strike Ivanti Connect Secure and Policy Secure Gateways Authentication Bypass	CWE: 287 CVE: 2023-46805	This strike exploits an authentication bypass vulnerability has been reported in Ivanti Connect Secure (formerly Pulse Secure) and Ivanti Policy Secure Gateways. This vulnerability is due to insufficient validation of HTTP request paths in the web process. A remote, unauthenticated attacker can exploit this vulnerability by using one of the Request-URI prefixes and pivoting to a second endpoint. Successful exploitation could result in unauthenticated access to some authenticated REST API endpoints.
Strike QNAP VioStor NVR OS command injection	CWE: 78 CVE: 2023-47565	This strike exploits an OS command injection vulnerability in QNAP VioStor NVR models running QVR Firmware 4.x. The vulnerability is due to improper validation of user-supplied data. A remote, authenticated attacker can exploit this vulnerability by submitting a crafted request to the target server. Successful exploitation could result in remote code execution in the context of the running sever.
Strike Apache OFBiz XMLRPC Insecure Deserialization CVE 2023-49070	CWE: 94 CVE: 2023-49070	This strike exploits an insecure deserialization vulnerability in Apache OFBiz. This vulnerability is due to the unmaintained XML-RPC library which deserializes user data. A remote, unauthenticated attacker could exploit this vulnerability by sending a request to the server with an encoded or unnormalized request URI to the "xmlrpc" endpoint, an empty USERNAME or PASSWORD parameter with a parameter requirePasswordChange with a value of Y, and a crafted Java object in a serializable XML element. Successfully exploiting this vulnerability could result in remote code execution in the security context of the user running the OFBiz server.
Strike ownCloud Graph API Information Disclosure Vulnerability	CWE: 22 CVE: 2023-49103	This strike exploits an information disclosure vulnerability in the ownCloud Graph API extension. The vulnerability exists because the affected versions rely on a third-party GetPhpInfo.php library that exposes the secrets stored in environment variables. This flaw allows attackers to steal sensitive information like admin passwords, mail server credentials, and license keys. A remote attacker could exploit the vulnerability by sending a crafted request to the target service. Successful exploitation could result in the disclosure of sensitive information.
Strike Apache Struts HttpParameters.java Unrestricted File Upload	CWE: 552 CVE: 2023-50164	This strike exploits a directory traversal vulnerability in Apache Struts framework. The vulnerability is due to insufficient validation of HTTP parameters during file uploads to the "upload.action" endpoint, resulting in unrestricted file uploads. The vulnerability allows an attacker to manipulate file upload parameters to enable path traversal and upload a malicious file to the target server leading to remote code execution, gaining full system control. *NOTE: While running the strike in one-arm mode, poc.txt file gets created in the /tmp directory of the vulnerable server.
Strike Apache OFBiz Authentication Bypass	CWE: 918 CVE: 2023-51467	This strike exploits an authentication bypass vulnerability in Apache OFBiz. This vulnerability is due to improper input validation of the credentials by the checkLogin function. A remote, unauthenticated attacker could exploit this vulnerability by sending a request with null or invalid username and password parameters and the requirePasswordChange parameter as Y to the server. Successfully exploiting this vulnerability could result in remote code execution in the security context of the web server running the vulnerable application.

Name	References	Description
Strike Apache Kafka Groovy Script Remote Code Execution	CWE: 94 CVE: 2023-52251	This strike exploits a command injection vulnerability in the web component of Apache Kafka. The vulnerability is due to unrestricted Groovy script execution within the smart filter functionality. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request and might result in arbitrary command execution under the security context of the kafkaui user.
Strike WordPress Backup Migration Plugin Remote Code Execution Vulnerability	CVE: 2023-6553	This strike exploits a remote code execution vulnerability in the WordPress Backup Migration plugin. The vulnerability arises from improper input validation in the backup-heart.php script. A remote, unauthenticated attacker could leverage this flaw by sending a specially crafted HTTP POST request, potentially leading to the execution of arbitrary PHP code on the target server.
Strike MLflow get-artifact Local File Read Vulnerability	CWE: 29 CVE: 2023-6909	This strike exploits a Local File Inclusion (LFI) vulnerability in the MLflow framework, which is hosted in the GitHub repository mlflow/mlflow. MLflow is a platform designed to streamline machine learning development, including tracking experiments, packaging code into reproducible runs, and sharing and deploying models. The vulnerability arises from improper handling of URL paths containing directory traversal characters when associating runs with experiments, allowing remote unauthenticated attackers to read arbitrary files on the server. The issue arises from a URI parsing confusion, which allows attackers to manipulate the artifact_location parameter during the creation of an experiment. This can lead to the unintended inclusion of sensitive files like /etc/passwd. Successful exploitation could result in the disclosure of sensitive information.
Strike Palo Alto Networks PAN-OS Management Interface Authentication Bypass	CWE: 306 CVE: 2024-0012	This strike exploits a Authentication Bypass vulnerability in Palo Alto Networks PAN-OS. The vulnerability is due to missing authentication to a critical path. A remote, unauthenticated attacker can exploit by sending a crafted HTTP request to the management web interface. Successful exploitation could result in information disclosure.
Strike Centreon Web updateDirectory SQL Injection Vulnerability	CVE: 2024-0637	This strike exploits an SQL injection vulnerability in the Centreon Web module. The vulnerability exists due to improper input validation in the updateDirectory function when processing the dir_id parameter. A remote, authenticated attacker could leverage this flaw by sending a specially crafted request, leading to arbitrary SQL command execution on the target database.
Strike Progress Kemp LoadMaster REST API Improper Input Validation	CVE: 2024-1212 CWE: 78	This strike exploits an Improper Input Validation Vulnerability against Progress Kemp LoadMaster. This vulnerability is due to improper user input validation when processing REST API requests. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to a target server. Successful exploitation can lead to arbitrary command execution.
Strike ConnectWise ScreenConnect SetupModule Authentication Bypass	CWE: 288 CVE: 2024-1709	This strike exploits an authentication bypass vulnerability in ConnectWise ScreenConnect. The vulnerability is due to improper validation of a request URL. A remote attacker could exploit this vulnerability by sending a crafted request to the target server, which will not match the expected value and the comparison will return false, allowing processing of the request to continue. Successful exploitation could result in privilege escalation.

Name	References	Description
Strike Atlassian Confluence Data Center and Server addlanguage Remote Code Execution	CWE: 94 CVE: 2024-21683	This strike exploits a remote code execution vulnerability in the Confluence Data Center and Server. The vulnerability is due to insufficient input validation in the function that allows users to add new code block macro language definitions. This flaw allows an authenticated attacker to inject and execute arbitrary Java code by uploading a malicious language file. A remote, authenticated attacker could leverage this vulnerability to inject Java code, resulting in arbitrary code execution under the security context of the user running the vulnerable application. *Note : While running the strike in one-arm mode, it creates a file /tmp/test on the target server.
Strike Ivanti Connect Secure and Policy Secure Gateways Command Injection	CWE: 77 CVE: 2024-21887	This strike exploits a command injection vulnerability in the web components of Ivanti Connect Secure and Ivanti Policy Secure Gateways. This vulnerability is due to the insufficient validation of HTTP arguments. In the web application, two different paths are susceptible to system command injection. The user-submitted data is directly employed in the Python Popen function without undergoing any sanitization. Consequently, an attacker can inject ";command;" and execute shell commands. A remote authenticated attacker could exploit this vulnerability by sending a crafted request to a target server. Successful exploitation could result in arbitrary shell command execution under the security context of the root user.
Strike Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery Vulnerability	CWE: 918 CVE: 2024-21893	This strike exploits a Server Side Request Forgery (SSRF) vulnerability in the SAML component of Ivanti Connect Secure, Ivanti Policy Secure, and Ivanti Neurons. The vulnerability arises from insufficient validation of XML content processed by the SAML server, which utilizes an outdated xmltooling library. The URI attribute of the RetrievalMethod element of the XML SOAP allows requests for remote resources via an HTTP GET request, leading to SSRF attacks. A remote, unauthenticated attacker could exploit this vulnerability to access restricted resources. This vulnerability when chained with CVE-2024-21887 may lead to remote code execution.
Strike Centreon Web updateLCARelation SQL Injection Vulnerability	CVE: 2024-23116	This strike exploits an SQL injection vulnerability in the Centreon Web module. The vulnerability exists due to insufficient input validation in the updateLCARelation function when processing the acl_r_topos parameter. A remote, authenticated attacker could leverage this flaw to execute arbitrary SQL commands on the target server's database.
Strike Centreon Web updateContactServiceCommands SQL Injection Vulnerability	CVE: 2024-23117	This strike exploits an SQL injection vulnerability in the Centreon Web module. The vulnerability exists due to insufficient input validation in the updateContactServiceCommands function when processing the contact_svNotifCmds[] parameter. Exploiting this vulnerability allows a remote, authenticated attacker to execute arbitrary SQL commands on the target database, potentially compromising its integrity and security.

Name	References	Description
Strike Rejetto HTTP File Server Template Injection Vulnerability	CWE: 94 CVE: 2024-23692	This strike exploits a server-side template injection vulnerability in Rejetto HTTP File Server. The vulnerability arises from improper handling of the search query parameter within the server's default template, which processes user-supplied content without adequate escaping. Attackers can exploit this flaw to inject arbitrary macros or commands, potentially compromising the system. Successful exploitation allows unauthenticated remote attackers to execute code with the privileges of the user running the HFS server.
Strike Windows CreateProcess cmd.exe Command Injection Vulnerability	CWE: 78 CVE: 2024-24576 CVE: 2024-1874 CVE: 2024-3566	This strike exploits a command injection vulnerability in Windows. The vulnerability arises from improper escaping of arguments when invoking batch files ('bat' and 'cmd' extensions) by the standard libraries across various programming languages. As a result, the Windows command shell (cmd.exe) can be manipulated into executing malicious code. Multiple CVEs are tied to this vulnerability (CVE-2024-24576, CVE-2024-3566, CVE-2024-1874, CVE-2024-22423), however, they all exploit the same underlying weakness. A remote, unauthenticated attacker could exploit this vulnerability by controlling the arguments passed to the spawned process. Successful exploitation could lead to the execution of arbitrary shell commands, bypassing the escaping mechanism, and operating within the security context of the target server.
Strike Check Point Quantum Security Gateways Information Disclosure Vulnerability	CWE: 200 CVE: 2024-24919	This strike exploits a directory traversal vulnerability in Check Point Quantum Security Gateways, affecting systems with Remote Access VPN or Mobile Access Software Blades enabled. The vulnerability is due to improper sanitization and validation of user input in the '/clients/MyCRL' endpoint. A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted POST request to the vulnerable endpoint containing the string 'CSHELL/' and a path traversal sequence, which could disclose sensitive information, including files containing password hashes.
Strike JetBrains TeamCity BaseController Authentication Bypass Vulnerability	CWE: 288 CVE: 2024-27198	This strike exploits an authentication bypass vulnerability in JetBrains TeamCity. The vulnerability is due to an authentication weakness in the BaseController class, which allows unauthenticated users to access restricted endpoints. It results from inadequate validation of parameters such as the "jsp" parameter and the ".jsp" extension in URLs. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server. Successful exploitation could result in an attacker bypassing the server's authentication mechanisms, in the worst case, leading to remote code execution under the security context of the target server.
Strike JetBrains TeamCity Authentication Bypass Vulnerability	CWE: 23 CVE: 2024-27199	This strike exploits an authentication bypass vulnerability in JetBrains TeamCity. This vulnerability allows an unauthenticated attacker to access certain authenticated endpoints without proper authentication. By exploiting path traversal issues in specific paths like /res/, /update/, and /.well-known/acme-challenge/, an attacker can reach sensitive JSP pages and servlet endpoints, leading to information disclosure and potential modification of system settings. A remote, unauthenticated attacker could execute denial-of-service attacks by changing the HTTPS port number or uploading a certificate that fails client-side validation, potentially enabling eavesdropping or man-in-the-middle attacks.

Name	References	Description
Strike Apache HugeGraph-Server Improper Access Control Vulnerability	CWE: 284 CVE: 2024-27348	This strike exploits an improper access control vulnerability in Apache Hugegraph. The flaw exists in the Gremlin query language endpoint. Improper validation and insufficient filtering of reflection methods allow attackers to bypass sandbox restrictions and execute arbitrary code remotely. A remote, unauthenticated attacker could exploit this vulnerability by crafting a malicious Gremlin query that bypasses security checks in the HugeGraph Server. *Note : While running the strike in one-arm mode, it creates a file /tmp/poc on the target server.
Strike SolarWinds Web Help Desk Hard-Coded Credentials	CWE: 798 CVE: 2024-28987	This strike exploits an information disclosure vulnerability in SolarWinds Web Help Desk. This vulnerability is due to hardcoded credentials. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted request to the target server and could result in information disclosure.
Strike SolarWinds Serv-U Path Traversal Vulnerability	CWE: 22 CVE: 2024-28995	This strike exploits a directory traversal vulnerability in the SolarWinds Serv-U file transfer solution. The vulnerability arises due to improper validation of two user input HTTP parameters InternalDir and InternalFile. These parameters are checked for directory traversal sequences but fail to account for different path separators. Attackers can exploit this by using forward slashes instead of backslashes, and vice versa, bypassing the check and allowing traversal to arbitrary directories. This vulnerability enables remote, unauthenticated attackers to access sensitive files and potentially further compromise the system.
Strike MLflow URI Parsing Confusion Local File Read Vulnerability	CWE: 29 CVE: 2024-2928	This strike exploits a Local File Inclusion (LFI) vulnerability in the MLflow framework, which is hosted in the GitHub repository mlflow/mlflow. The vulnerability arises from improper handling of URL paths containing directory traversal characters when associating runs with experiments, allowing remote unauthenticated attackers to read arbitrary files on the server. A remote, unauthenticated attacker can exploit this flaw by manipulating the fragment part of the URI to read arbitrary files on the local file system, including sensitive files like '/etc/passwd'. The vulnerability is a bypass to a previous patch CVE-2023-6909 that addressed similar manipulation within the URI's query string. Successful exploitation could result in the disclosure of sensitive information.
Strike Ivanti Endpoint Manager (EPM) xp_cmdshell SQL Injection Vulnerability	CWE: 89 CVE: 2024-29824	This strike exploits an SQL injection vulnerability in Ivanti Endpoint Manager (EPM). The vulnerability lies in the RecordGoodApp() function, where an unsanitized md5 value provided by the user is used in an SQL query. Attackers can exploit this by sending a crafted SOAP request, injecting SQL commands, such as xp_cmdshell, to execute malicious code. Successful exploitation of this vulnerability could allow an unauthenticated attacker within the same network to execute arbitrary code.
Strike Apache OFBiz Path Traversal Vulnerability	CWE: 22 CVE: 2024-32113	This strike exploits a path traversal vulnerability in Apache OFBiz. The vulnerability arises from inadequate sanitization of input at the vulnerable endpoint /webtools/control/forgotPassword. An attacker can exploit this endpoint to access the ProgramExport functionality, which can then be leveraged for remote code execution. Successful exploitation allows unauthenticated remote attackers to execute arbitrary code with the privileges of the user running the vulnerable server.

Name	References	Description
Strike D-Link nas_sharing Hardcoded Credentials	CVE: 2024-3272 CWE: 798	This strike exploits an authentication bypass vulnerability in D-Link NAS sharing. The vulnerability is due to the use of hardcoded credentials in nas_sharing. By sending a crafted request, an attacker can bypass authentication.
Strike D-Link nas_sharing Remote Code Execution	CVE: 2024-3273 CWE: 77	This strike exploits a command injection vulnerability in D-Link NAS sharing. The vulnerability is due to improper sanitization of user provided parameter in nas_sharing. By sending a crafted request, an attacker can execute arbitrary command on the system in the context of the running service.
Strike Palo Alto Networks PAN-OS Command Injection Vulnerability	CWE: 77 CVE: 2024-3400	This strike exploits a command injection vulnerability in Palo Alto Networks PAN-OS. The vulnerability is due to insufficient validation of user data by the GlobalProtect service. When parsing the SESSID cookie, the value is not verified to be a valid UUID. A remote, unauthenticated attacker could exploit this vulnerability by sending a crafted SESSID value, including directory traversal and shell command characters to the target service. Successful exploitation would result in the execution of arbitrary commands under the security context of the ROOT user.
Strike Adobe Commerce and Magento Improper Restriction of XML External Entity Reference (XXE) Vulnerability	CWE: 611 CVE: 2024-34102	This strike exploits an XML External Entity Injection vulnerability in Adobe Commerce and Magento. The vulnerability is due to improper validation during deserialization of user-supplied XML data. When deserializing XML payloads, the parser processes external entities embedded within the XML structure. A remote, unauthenticated attacker could exploit this vulnerability by injecting maliciously crafted XML that references external entities, enabling them to access or tamper with sensitive server-side data. Successful exploitation of this vulnerability could lead to disclosure of sensitive information.
Strike Apache OFBiz Directory Traversal Vulnerability	CVE: 2024-36104	This strike exploits a directory traversal vulnerability in Apache OFBiz. The vulnerability exists due to improper validation of URL data when processing HTTP requests. A remote, unauthenticated attacker can leverage this flaw by sending specially crafted requests, potentially bypassing authentication or executing arbitrary OS commands on the affected server.
Strike OSGeo GeoServer GeoTools Eval Injection Vulnerability	CWE: 94 CVE: 2024-36401	This strike exploits a command injection vulnerability in Geoserver. The vulnerability arises from the unsafe evaluation of XPath expressions in the GeoTools library. This evaluation is erroneously applied to both complex and simple feature types, making all GeoServer instances vulnerable. The vulnerability can be exploited through various OGC (Open Geospatial Consortium) request parameters like WFS GetPropertyValue. Successful exploitation of this vulnerability could lead to unauthenticated remote code execution on the affected GeoServer instances, potentially leading to full server compromise. *Note : While running the strike in one-arm mode, it creates two files /tmp/test1 and /tmp/test2 on the target server.

Name	References	Description
Strike Apache OFBiz ProgramExport Incorrect Authorization Vulnerability	CWE: 863 CVE: 2024-38856	This strike exploits an incorrect authorization vulnerability in Apache OFBiz. The vulnerability arises from a logic flaw in the authentication of endpoints. Authentication is performed on the requestUri, which points to an endpoint that does not require authentication, such as 'forgotPassword'. However, the page located at overrideViewUri is rendered instead. This flaw allows unauthenticated access to the ProgramExport endpoint by chaining it with any other endpoints that do not require authentication. By leveraging this override view functionality, an attacker can achieve remote code execution. Successful exploitation allows unauthenticated remote attackers to execute arbitrary code with the privileges of the user running the vulnerable server. *Note: While running the strike in one-arm mode, it creates a file /tmp/test on the vulnerable server.
Strike CrushFTP Server Side Template Injection Vulnerability	CWE: 94 CVE: 2024-4040	This strike exploits a server side template injection vulnerability in CrushFTP. The vulnerability arises from inadequate input validation and improper handling of user-supplied data in the code responsible for variable replacement in API responses, enabling attackers to inject and execute arbitrary templates. To exploit the vulnerability, attackers can leverage the server-side templating engine of CrushFTP by injecting malicious templates into API responses. This allows an unauthenticated remote attacker to read files from the file system outside of the Virtual File System (VFS) Sandbox, bypass authentication to gain administrative access, and perform remote code execution on the server.
Strike Veertu Anka Build Directory Traversal Vulnerability	CVE: 2024-41163	This strike exploits a directory traversal vulnerability in Veertu Anka Build. The vulnerability exists due to insufficient validation of the "service" parameter in the archive API endpoint. A remote, unauthenticated attacker could leverage this flaw by sending a specially crafted request, enabling them to access and read arbitrary files from the target server.
Strike Mitel MiCollab Path Traversal Vulnerability	CWE: 22 CVE: 2024-41713	This strike exploits a path traversal vulnerability in Mitel MiCollab. A remote unauthenticated attacker can conduct a path traversal attack due to insufficient input validation. Successful exploitation could allow unauthorized access, and the ability to read arbitrary files on the server.
Strike Apache OFBiz Forced Browsing Vulnerability	CWE: 425 CVE: 2024-45195	This strike exploits a forced browsing vulnerability in Apache OFBiz. The vulnerability is due to improper access control in the web application. A remote attacker could exploit this vulnerability by sending a crafted HTTP POST request to the targeted server. Successful exploitation could result in unauthorized access to sensitive information.
Strike PHP-CGI OS Command Injection Vulnerability	CWE: 78 CVE: 2024-4577	This strike exploits an OS command injection vulnerability in PHP-CGI on Windows. The vulnerability is due to the improper handling of character encoding conversions within the Windows operating system, particularly the "Best Fit" feature to replace characters in command line given to Win32 API functions. The PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to the PHP binary being run. As a result, remote, unauthenticated attackers can inject arguments into the PHP CGI process, leading to arbitrary code execution.

Name	References	Description
Strike ServiceNow Improper Input Validation Vulnerability	CWE: 1287 CVE: 2024-4879	This strike exploits a Jelly template injection vulnerability in ServiceNow platform. The vulnerability arises from improper input validation in the Jelly scripting engine, which is used within ServiceNow for rendering dynamic content. A remote, unauthenticated attacker can exploit this vulnerability by crafting a malicious input that the Jelly engine processes incorrectly, leading to remote code execution. Successful exploitation can result in complete compromise of the affected ServiceNow instance, allowing attackers to execute arbitrary commands, access sensitive information, and potentially manipulate system settings.
Strike Aviatrix Controller OS Command Injection Vulnerability	CVE: 2024-50603 CWE: 78	This strike exploits an OS command injection vulnerability in Aviatrix Controller. The vulnerability allows unauthenticated remote attackers to inject shell metacharacters into the /v1/api endpoint via the cloud_type parameter in list_flightpath_destination_instances or the src_cloud_type parameter in flightpath_connection_test. Successful exploitation of the vulnerability allows remote attackers to execute arbitrary commands on the affected system.
Strike Cleo Harmony VLTrader Lexicom File Upload Vulnerability	CVE: 2024-50623 CWE: 434	This strike exploits a file upload vulnerability in Cleo Harmony, VLTrader, Lexicom. The vulnerability allows unauthenticated attackers to upload malicious files, which can then be exploited via directory traversal to execute arbitrary code. Successful exploitation of this vulnerability allows remote attackers to access sensitive information, modify data, or disrupt system operations.
Strike Cyber Panel Getresetstatus Remote Code Execution	CWE: 78 CVE: 2024-51378	This strike exploits a command injection vulnerability in the web component of Cyber Panel. The vulnerability is due to missing authentication for critical function. The getresetstatus endpoint of CyberPanel allows remote unauthenticated attackers to execute arbitrary commands by bypassing secMiddleware protections. The vulnerability can be exploited using shell metacharacters in the statusfile parameter. Successful exploitation could result in arbitrary command execution under the security context of the root user.
Strike Cyber Panel upgrademysqlstatus Remote Code Execution	CWE: 306 CVE: 2024-51567	This strike exploits a command injection vulnerability in the web component of Cyber Panel. The vulnerability is due to missing authentication for critical function. The upgrademysqlstatus endpoint of CyberPanel allows remote unauthenticated attackers to execute arbitrary commands by bypassing secMiddleware protections, which only filter POST requests. The vulnerability can be exploited using shell metacharacters in the statusfile parameter. Successful exploitation could result in arbitrary command execution under the security context of the root user.
Strike ServiceNow Incomplete List of Disallowed Inputs Vulnerability	CWE: 697 CVE: 2024-5217	This strike exploits a Jelly template injection vulnerability in ServiceNow platform. The vulnerability arises from improper input validation in the Jelly scripting engine, which is used within ServiceNow for rendering dynamic content. A remote, unauthenticated attacker can exploit this vulnerability by providing crafted malicious input that the Jelly engine processes incorrectly. This leads to the disclosure of sensitive information, including database details. Successful exploitation could result in unauthorized access to sensitive database details within the affected ServiceNow instance.

Name	References	Description
Strike Apache Struts FileuploadIntercept or Unrestricted File Upload	CWE: 434 CVE: 2024-53677	This strike exploits a file upload vulnerability in Apache Struts 2 framework. The vulnerability lies in the File Upload Interceptor, which allows attackers to exploit improperly sanitized file names containing path traversal sequences. This can lead to arbitrary file writes, enabling remote code execution (RCE) in vulnerable applications. The exploitation involves manipulating field name capitalization in file upload forms to bypass Struts 2's parameter binding, allowing attackers to control internal variables like top.uploadFileName via the OGNL value stack. Exploitation is customized, requiring knowledge of the upload endpoint's structure.
Strike Ivanti Cloud Services Appliance OS Command Injection Vulnerability	CWE: 78 CVE: 2024-8190	This strike exploits an OS command injection vulnerability in the Ivanti Cloud Services Appliance, versions prior to 4.6 Patch 519. This vulnerability is due to improper validation of user data sent to the datetime php endpoint. Successful exploitation might result in arbitrary code execution in the context of the root user.
Strike Ivanti Cloud Services Appliance broker Authentication Bypass	CWE: 22 CVE: 2024-8963	This strike exploits Authentication Bypass vulnerability in Ivanti Cloud Services Appliance. A remote, unauthenticated attacker could exploit this vulnerability by sending crafted requests to the target server. Successful exploitation could allow an unauthorized attacker to access restricted functionality.
Strike Palo Alto Networks Expedition OS Command Injection Vulnerability	CVE: 2024-9463 CWE: 78	This strike exploits an OS command injection vulnerability in Palo Alto Networks Expedition. The vulnerability is due to lack of neutralization of special elements used in OS commands. A remote unauthenticated attacker can exploit this vulnerability by running arbitrary OS commands as root. Successful exploitation of this vulnerability could lead to remote code execution.
Strike Langflow Code Validation Missing Authentication Vulnerability	CWE: 94 CVE: 2025-3248	This strike exploits a missing authentication vulnerability in Langflow. The vulnerability is due to lack of authentication in /api/v1/validate/code endpoint. A remote, unauthenticated attacker could exploit this vulnerability by embedding malicious Python code in function decorator or default argument. Successfully exploiting this vulnerability can lead to execution of arbitrary code under the security context of the service.
Strike CVSTrac FileDiff v2 Parameter Command Execution	CVE: 2004-1456 BID: 10878	This strike exploits an arbitrary command execution vulnerability in CVSTrac. The vulnerability is due to failure to properly sanitize user-supplied input to the rcsinfo parameter. A remote attacker could execute arbitrary commands on the target system by sending shell metacharacters in a web request.
Strike Cybozu ag.exe id Parameter Directory Traversal	BID: 19733 CVE: 2006-4490	This strike exploits a directory traversal vulnerability in the Cybozu web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Cybozu s360.exe id Parameter Directory Traversal Variant 1	BID: 19733  CVE: 2006-4490	This strike exploits a directory traversal vulnerability in the Cybozu web application.
Strike Cybozu s360.exe id Parameter Directory Traversal Variant 2	BID: 19733  CVE: 2006-4490	This strike exploits a directory traversal vulnerability in the Cybozu web application.
Strike Data Dynamics ActiveX Save Method Arbitrary File Write	CVE: 2007-3883  BID: 24959	This strike exploits an arbitrary file write bug in the Data Dynamics ActiveX control when calling the Save method.
Strike Data Dynamics ActiveX SaveLayoutChanges Method Arbitrary File Write	CVE: 2007-3883  BID: 24959	This strike exploits an arbitrary file write bug in the Data Dynamics ActiveX control when calling the SaveLayoutChanges method.
Strike Data Dynamics ActiveX SaveMenuUsageData Method Arbitrary File Write	CVE: 2007-3883  BID: 24959	This strike exploits an arbitrary file write bug in the Data Dynamics ActiveX control when calling the SaveMenuUsageData method.
Strike DBGuestBook utils.php dbs_base_path Parameter PHP File Include	CWE: 94  CVE: 2007-1165  BID: 22658	This strike exploits a PHP include flaw in the DBGuestBook application.
Strike DBGuestBook guestbook.php dbs_base_path Parameter PHP File Include	CWE: 94  CVE: 2007-1165  BID: 22658	This strike exploits a PHP include flaw in the DBGuestBook application.
Strike DBGuestBook views.php dbs_base_path Parameter PHP File Include	CWE: 94  CVE: 2007-1165  BID: 22658	This strike exploits a PHP include flaw in the DBGuestBook application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Dell KACE K1000 krash rpt OS Command Injection	EXPLOITDB : 46684	An OS command injection vulnerability exists in Dell KACE K1000 versions before 6.4.120822, due to lack of sanitization of user-supplied data. By sending a crafted 'kuid' parameter in a HTTP request to '/service/krash rpt.php', a remote unauthenticated attacker may execute arbitrary OS commands as the user 'www'.
Strike DivX ActiveX Browser Plugin Denial of Service	BID: 22133  CVE: 2007-0429	This strike causes a denial of service in the DivX browser plugin's ActiveX control.
Strike D-Link DAP-1160 Authentication Bypass		A vulnerability exists in the D-Link DAP-1160 wireless access point that allows an attacker to gain unauthorized access to the administration page if the first url accessed in the first 40 seconds since the device web server has started is the url <a href="http://IP_ADDR/tools_firmw.htm">http://IP_ADDR/tools_firmw.htm</a> . This is especially dangerous since a separate vulnerability exists in the same device that allows an unauthenticated user to run commands remotely, such as rebooting the device (strike-id E10-0fa01).
Strike D-Link DIR8xx Information Disclosure	EXPLOITDB : 42729	This strike exploits a information disclosure vulnerability in D-Link DIR-8xx Wired/Wireless Router. This vulnerability is due to improper handling of key-value pairs sent through HTTP POST requests. By exploiting this vulnerability a remote, authenticated attacker can obtain sensitive data, including router credentials.
Strike Docker Daemon API Unauthorized Remote Code Execution		This strike exploits a remote code execution vulnerability in Docker daemon API. An attacker can start a docker container, attach host's /etc to the container and read/write files in etc.
Strike BerliOS Docpile we folder.class.php INIT_PATH Parameter PHP File Include	BID: 19428  CVE: 2006-4075	This strike exploits a PHP include flaw in the berliOS Docpile:we web application.
Strike BerliOS Docpile we email.inc.php INIT_PATH Parameter PHP File Include	BID: 19428  CVE: 2006-4075	This strike exploits a PHP include flaw in the berliOS Docpile:we web application.
Strike BerliOS Docpile we document.class.php INIT_PATH Parameter PHP File Include	BID: 19428  CVE: 2006-4075	This strike exploits a PHP include flaw in the berliOS Docpile:we web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike BerliOS Docpile we auth.inc.php INIT_PATH Parameter PHP File Include	BID: 19428 CVE: 2006-4075	This strike exploits a PHP include flaw in the berliOS Docpile:we web application.
Strike BerliOS Docpile we access.inc.php INIT_PATH Parameter PHP File Include	CVE: 2006-4076	This strike exploits a PHP include flaw in the berliOS Docpile:we web application.
Strike BerliOS Docpile we folders.inc.php INIT_PATH Parameter PHP File Include	CVE: 2006-4076	This strike exploits a PHP include flaw in the berliOS Docpile:we web application.
Strike BerliOS Docpile we init.inc.php INIT_PATH Parameter PHP File Include	CVE: 2006-4076	This strike exploits a PHP include flaw in the berliOS Docpile:we web application.
Strike BerliOS Docpile we templates.inc.php INIT_PATH Parameter PHP File Include	CVE: 2006-4076	This strike exploits a PHP include flaw in the berliOS Docpile:we web application.
Strike Dolibarr ERP-CRM rowid SQL Injection	EXPLOITDB : 46095	This strike exploits an SQL injection vulnerability in Dolibarr ERP-CRM. The vulnerability is due to the improper sanitization of requests sent to the application. An attacker could exploit this by sending a specifically crafted 'rowid' parameter, potentially resulting in the execution of SQL commands which may lead to information disclosure.
Strike Microsoft DXMedia SDK 6 SourceUrl ActiveX Remote Code Execution	CVE: 2007-4336 BID: 25279	This strike exploits a vulnerability in a DXMedia ActiveX control.
Strike Easy File Sharing Web Server - sendmail.ghp Stack Buffer Overflow	EXPLOITDB : 42165	This strike exploits a stack buffer overflow vulnerability in Easy File Sharing Web Server. The vulnerability is due to a lack of boundary checking on user input when requesting sendmail.ghp resource. By exploiting this vulnerability, an attacker could execute arbitrary code in the security context of user. NOTE: Strike will launch calc.exe when run in OneArm mode. Verified against Easy File Sharing Web Server Version 7.2 running on Windows 7 x86 with DEP and ASLR disabled.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Easy File Sharing Web Server - vfolder.ghp Stack Buffer Overflow	EXPLOITDB : 42261	This strike exploits a stack buffer overflow vulnerability in Easy File Sharing Web Server. The vulnerability is due to a lack of boundary checking on user input when requesting vfolder.ghp resource. By exploiting this vulnerability, an attacker could potentially execute arbitrary code in the security context of user. NOTE: Strike will launch calc.exe when run in OneArm mode. Verified against Easy File Sharing Web Server Version 7.2 running on Windows 7 x86 with DEP disabled.
Strike EasyMail Object EMSMTP.DLL ActiveX Control Buffer Overflow	CWE: 119 CVE: 2007-4607 BID: 25467	This module exploits a buffer overflow in the EasyMail Object EMSMTP.DLL ActiveX Control.
Strike EMail Security Virtual Appliance Remote Code Execution		This strike exploits a failure to validate user-supplied data to execute remote instructions in an ESVA VM.
Strike Empire CMS checklevel.php check_path Parameter PHP File Include	CVE: 2006-4354 BID: 19655	This strike exploits a PHP include flaw in the Empire CMS web application.
Strike Electric Sheep Fencing pfSense Code Execution Vulnerability		This strike exploits a code execution vulnerability inside Electric Sheep Fencing pfSense. The vulnerability is due to improper HTTP POST parameter validation by the web interface. By exploiting this vulnerability an attacker could execute malicious scripts on the target machine.
Strike Microsoft Excel NULL Pointer DoS (A) (HTTP)	BID: 22717 CVE: 2007-1239	This strike exploits a denial of service flaw in Microsoft Excel using a corrupted XLS document.
Strike Microsoft Excel NULL Pointer DoS (B) (HTTP)	BID: 22717 CVE: 2007-1239	This strike exploits a denial of service flaw in Microsoft Excel using a corrupted XLS document.
Strike Drupal RESTful Web Services Module Default Page Callback Function Remote php Command Execution	EXPLOITDB : 40130	This strike exploits a command execution in the Drupal RESTful Web Services (RESTWS) Module. The RESTWS module checks requests to see if it references a callback function. If it does not have a default callback function, other arguments in the URL are handled as arguments, including an argument which is used as the callback function. This argument can be set to "system," allowing for command execution. An attacker can send a specially crafted HTTP request to achieve remote php command execution. Successful exploitation can result in the execution of arbitrary code with the privileges of the target Drupal server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike TOPSEC Firewall ELCO ELIGIBLECONTEST ANT Recon Probe	EXPLOITDB : 40272	This strike emulates a reconnaissance attack against TopSec Firewalls. This attack attempts several command executions to retrieve information from the target system. NOTE: By default the vulnerable services are accessed via SSL connection (port 443). A publicly available exploit for this vulnerability can be found in the reported leak of 0Day exploits from the NSA by a group known as the "Shadow Brokers", identified as ELIGIBLECONTESTANT.
Strike TOPSEC Firewall ELCO ELIGIBLECONTEST ANT Remote Code Execution	EXPLOITDB : 40272	This strike emulates a remote code execution attack against TopSec Firewalls. This attack uploads and executes arbitrary code via an HTTP POST request to /cgi/maincgi.cgi. NOTE: By default the vulnerable services are accessed via SSL connection (port 443). A publicly available exploit for this vulnerability can be found in the reported leak of 0Day exploits from the NSA by a group known as the "Shadow Brokers", identified as ELIGIBLECONTESTANT
Strike TOPSEC Firewall ELCA ELIGIBLECANDIDA TE Remote Code Execution	EXPLOITDB : 40273	This strike emulates a remote code execution attack against TopSec Firewalls. This attack uploads and executes arbitrary code via an HTTP POST request to /cgi/maincgi.cgi. NOTE: By default the vulnerable services are accessed via SSL connection (port 443). A publicly available exploit for this vulnerability can be found in the reported leak of 0Day exploits from the NSA by a group known as the "Shadow Brokers", identified as ELIGIBLECANDIDATE.
Strike FreePBX config display Parameter SQL Injection	EXPLOITDB : 40312	This strike exploits a SQL injection vulnerability in FreePBX. HTTP requests to /admin/config.php are not sanitized for SQL injection characters. A specially crafted HTTP request with a sql injection in the display parameter can be used to achieve arbitrary SQL statement execution, which can lead to arbitrary code execution with the mysql user privileges.
Strike WordPress Quizlord plugin Reflected Cross Site Scripting	EXPLOITDB : 45307	This strike exploits a reflected cross-site scripting vulnerability found in Quizlord WordPress plugin. This vulnerability is due to inadequate input filtering in the web interface, while parsing input passed to quiz title parameter. By exploiting this vulnerability an attacker could cause arbitrary HTML/script code to be executed by the target user's browser.
Strike Windows Explorer ICO File Format Divide by Zero	BID: 24346  CVE: 2007-2237	This strike exploits a denial of service flaw in the Windows Explorer using a Windows icon file (ICO) with an image height field set to zero.
Strike Facebook PhotoUploader 4 Buffer Overflow	CWE: 119  CVE: 2008-0660  BID: 27576	This strike exploits a buffer overflow vulnerability present in the Facebook ImageUploader ActiveX library created by Aurigma, and used by Facebook, MySpace, and others. Due to an issue involving improper bounds-checking, a malicious web page can use the ExtractIptc and ExtractExif functions to overflow the buffer, leading to system instability and the possibility of remote code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike FCRing FCRing.php s_fuss Parameter PHP File Include	CVE: 2007-1133  BID: 22693	This strike exploits a PHP include flaw in the FCRing web ring application.
Strike FireEye OS Remote File Disclosure	EXPLOITDB : 38090	This strike exploits a remote file disclosure vulnerability in FireEye OS. The vulnerability is due to improper filtering of HTTP parameters. By using a specially crafted GET request an attacker can cause the web server to return the contents of arbitrary files. NOTE: This strike runs by default over SSL (port 443).
Strike Firefox Array.reduceRight Integer Overflow	CWE: 189  CVE: 2011-2371  BID: 48372	This strike exploits an integer overflow vulnerability in Mozilla Firefox <= 3.6.18 that occurs when using the reduceRight method on an array with a very large length.
Strike Firefox Asynchronous Event Memory Corruption	CWE: 264  CVE: 2006-4253  BID: 19488	This strike exploits a flaw in Firefox that results in the corruption of memory and denial of service
Strike Mozilla Firefox SVG Surface Integer Overflow	CVE: 2006-0297  BID: 16476	This strike exploits a memory corruption vulnerability in Mozilla Firefox that occurs when a specific surface size is used in a SVG image.
Strike Incorrect libpng Usage (Extra Row) Heap Overflow	BID: 41174  CWE: 119  CVE: 2010-1205	This strike exploits a vulnerability in the way applications make use of the libpng library. Libpng uses callbacks to inform the application that data has been parsed and is available. If an application using libpng does not keep track of the number of rows parsed in the callbacks and continues to write the parsed pixel data into a buffer, a heap overflow can occur. Firefox (1.5.x and up) and Google Chrome (all) are known to be vulnerable.
Strike Mozilla Firefox CSS Border Width Memory Corruption	CWE: 119  CVE: 2006-1739  BID: 17516	This strike exploits a vulnerability in Mozilla Firefox when handling CSS that specifies large values for borders.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Mozilla Firefox CSS Layout Memory Corruption	CVE: 2007-3734 BID: 24946	This strike exploits a memory corruption vulnerability in Mozilla Firefox when rendering HTML that tries to reference deleted style information for a parent block.
Strike Firefox nsTreeContentView Use After Free	CWE: 399 CVE: 2010-0176 BID: 39128	This strike triggers a use-after-free (dangling pointer) vulnerability in the Firefox web browser by including non-xul elements as children of a xul element. Versions prior to 3.6.2, 3.5.9, and 3.0.19 are vulnerable.
Strike Mozilla Firefox designMode Deleted Object Reference Denial of Service Variant 1	CWE: 399 CVE: 2006-1993 BID: 17671	This strike exploits a denial of service flaw in Mozilla Firefox when referencing a deleted controller context when designMode is enabled.
Strike Mozilla Firefox designMode Deleted Object Reference Denial of Service Variant 2	CWE: 399 CVE: 2006-1993 BID: 17671	This strike exploits a denial of service flaw in Mozilla Firefox when referencing a deleted controller context when designMode is enabled.
Strike Mozilla Firefox Design Mode Deleted Style Reference Memory Corruption	CVE: 2007-3734 BID: 24946	This strike exploits a memory corruption vulnerability in Mozilla Firefox when operating in design mode to edit objects with crafted style attributes.
Strike Mozilla Firefox OBJECT Tag Crafted Style Null Dereference	CVE: 2007-3734 BID: 24946	This strike exploits a denial of service vulnerability in Mozilla Firefox when rendering an HTML OBJECT tag whose display style is set with a crafted value.
Strike Mozilla Firefox document.write() Buffer Overflow	CWE: 119 CVE: 2010-3179	This strike exploits a bug in Mozilla Firefox where using the document.write() method with extremely large messages can overflow a buffer and cause an arbitrary address to be written to the call stack.

Name	References	Description
Strike Firefox document.write() and appendChild() Memory Corruption	CWE: 119 CVE: 2010-3765 BID: 44425	This strike exploits a memory corruption vulnerability in Mozilla Firefox 3.5.15 and 3.6.12 that occurs when mixing calls to document.write() and node.appendChild().
Strike Mozilla Firefox escape() Return Value Memory Corruption	CWE: 94 CVE: 2009-2477 BID: 35660	This strike exploits a memory corruption in the Mozilla Firefox 3.5 Just-in-time Javascript compiler when calling the escape() function.
Strike Mozilla Firefox Floating Layer Column Layout Denial of Service	CVE: 2007-0775 BID: 22694	This strike exploits a denial of service condition in Mozilla Firefox when dynamically creating a new DOM node inside a floating layer with a columnar layout.
Strike Mozilla Firefox GeckoActiveXObject( ) Method Denial of Service	CVE: 2006-3803 BID: 19181	This strike exploits a memory corruption vulnerability in Mozilla Firefox when handling javascript that passes a long string to the GeckoActiveXObject() method.
Strike Mozilla Firefox HTML Frameset Dynamic Resize Memory Corruption	CWE: 119 CVE: 2007-2867 BID: 24242	This strike exploits a bug in Mozilla Firefox when modifying size attributes of a frameset dynamically.
Strike Firefox HTML URL Unicode Stack Overflow	BID: 31397 CWE: 119 CVE: 2008-0016	This strike exploits a stack overflow with an SEH overwrite in Firefox versions 2.0.0.16 and lower when an invalid URL segment is passed to ConvertUTF8toUTF16::write.
Strike Firefox Hyphenated URL Exploit Variant 2	BID: 14784 CVE: 2005-2871	This strike exploits a flaw in the Firefox browser that is triggered by a hostname in a URL that is all hyphens.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Mozilla Firefox-Thunderbird-SeaMonkey Javascript IDBKeyRange	BID: 53220 CWE: 399 CVE: 2012-0469	This strike exploits a use after free vulnerability in Mozilla Firefox/Thunderbird/SeaMonkey with IDBKeyRange object use after free.
Strike Mozilla Firefox InstallTrigger.install() Method Denial of Service	CWE: 399 CVE: 2006-1790 BID: 17516	This strike exploits a denial of service vulnerability in Mozilla Firefox when handling Javascript that calls the InstallTrigger.install() method.
Strike Mozilla Firefox Javascript UTF-8 Byte-order Marker Character Stripping	BID: 31346 CWE: 79 CVE: 2008-4065	This strike exploits a javascript parsing vulnerability in Mozilla Firefox. The browser incorrectly strips UTF-8 byte-order marker bytes when processing javascript.
Strike Mozilla Firefox Javascript Engine Function Arguments Memory Corruption	CWE: 189 CVE: 2006-3806 BID: 19181	This strike exploits a memory corruption vulnerability in Mozilla Firefox when handling Javascript code that passes many arguments to a function.
Strike Mozilla Firefox Javascript Engine ClearWatchPoint Memory Corruption	CWE: 119 CVE: 2007-0777 BID: 22694	This strike exploits a memory corruption vulnerability in Mozilla Firefox when handling Javascript that removes a watchpoint which is later referenced.
Strike Mozilla Firefox Javascript Engine 64k Atoms Memory Corruption	CWE: 119 CVE: 2007-0777 BID: 22694	This strike exploits a memory corruption vulnerability in Mozilla Firefox when handling Javascript code that contains more than 64k atoms.
Strike Mozilla Firefox Javascript Engine Object Getter Method Memory Corruption	CWE: 119 CVE: 2007-0777 BID: 22694	This strike exploits a memory corruption vulnerability in Mozilla Firefox when handling Javascript code involving calls to object getter methods for objects that have been garbage-collected.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Mozilla Firefox Javascript Engine Memory Corruption (Script.toSource)	CWE: 119 CVE: 2007-0777 BID: 22694	This strike exploits a memory corruption vulnerability in Mozilla Firefox when handling Javascript code that calls toSource() on a script object that has been compiled.
Strike Mozilla Firefox Javascript Engine Memory Corruption (Script.toString)	CWE: 119 CVE: 2007-0777 BID: 22694	This strike exploits a memory corruption vulnerability in Mozilla Firefox when handling Javascript code that calls toString() on a script object that has been compiled.
Strike Mozilla Firefox Event Handler Privilege Escalation	CVE: 2007-3737 BID: 24946	This strike exploits a privilege escalation flaw that allows DOM eventhandlers to run code with chrome privileges.
Strike Mozilla Firefox Javascript HTML Escaped Low Surrogate Characters	BID: 31346 CWE: 79 CVE: 2008-4066	This strike exploits a javascript parsing vulnerability in Mozilla Firefox. The browser incorrectly strips certain HTML-escaped low surrogate characters.
Strike Mozilla Firefox New Function Garbage Collection Denial of Service (Firefox Javascript SetPrivate)	CVE: 2006-3803 BID: 19181	This strike exploits a memory corruption vulnerability in Mozilla Firefox when handling Javascript that references a garbage-collected variable.
Strike Mozilla Firefox Javascript Large Regular Expression Parsing Memory Corruption	CWE: 189 CVE: 2006-1737 BID: 17516	This strike exploits a memory corruption vulnerability in Mozilla Firefox when parsing large regular expressions.
Strike Firefox CSS letter-spacing Property Memory Corruption (Privilege Escalation)	CVE: 2006-1734 BID: 17516	This strike exploits a vulnerability in Mozilla Firefox that permits Javascript code to access internal function objects.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Mozilla Firefox Javascript XBL.method.eval Variant 1	CWE: 264 CVE: 2006-1735 BID: 17516	This strike exploits a vulnerability in the Mozilla Firefox javascript engine that permits javascript to run scripts with local user permission.
Strike Mozilla Firefox Javascript XBL Compilation Scope Access	CWE: 264 CVE: 2006-1733 BID: 17516	This strike exploits a vulnerability in the Mozilla Firefox javascript engine that permits javascript to access the XBL compilation scope.
Strike Mozilla Firefox Javascript XBL Compilation Scope Access Variant 1	CWE: 264 CVE: 2006-1733 BID: 17516	This strike exploits a vulnerability in the Mozilla Firefox javascript engine that permits javascript to access the XBL compilation scope.
Strike Mozilla Firefox Javascript XBL Compilation Scope Access Variant 2	CWE: 264 CVE: 2006-1733 BID: 17516	This strike exploits a vulnerability in the Mozilla Firefox javascript engine that permits javascript to access the XBL compilation scope.
Strike Firefox Javascript Engine Multibyte Character Escape Heap Overflow	CVE: 2005-2705 BID: 14917	This strike exploits a vulnerability in the Firefox that is triggered when escaping multibyte-character strings in Javascript.
Strike Mozilla Firefox Javascript Engine XML Parser Integer Overflow	CVE: 2006-0297 BID: 16476	This strike exploits a memory corruption vulnerability in Mozilla Firefox that occurs when a large number of elements are fed to the XML parser.
Strike Firefox CSS letter-spacing Property Memory Corruption (Letter Spacing)	CWE: 189 CVE: 2006-1730 BID: 17516	This strike exploits a memory corruption vulnerability in Mozilla Firefox when handling HTML which contains a CSS letter-spacing property whose value contains a large number.

Name	References	Description
Strike Firefox Link Tag Code Injection	BID: 13216 CWE: 94 CVE: 2005-1155	This strike exploits a flaw in the Firefox's handling of the link tag that allows arbitrary Javascript to execute with chrome privileges
Strike Firefox resource --Local File Read Variant 1	CVE: 2007-3073	This strike exploits a lack of input validation to read in arbitrary files with Firefox using the 'resource://gre/' protocol handler.
Strike Firefox resource --Local File Read Variant 2	CVE: 2007-3073	This strike exploits a lack of input validation to read in arbitrary files with Firefox using the 'resource://gre/' protocol handler.
Strike Firefox location.hostname Null Byte Vulnerability	BID: 22566 CWE: 264 CVE: 2007-0981	This strike allows access to third-party domain's cookies via a vulnerability in Firefox that allows a site to impersonate an arbitrary domain name
Strike Firefox LookupGetterOrSetter Dangling Pointer	CWE: 119 CVE: 2010-3183 BID: 44249	This strike triggers a vulnerability in Firefox < 3.5.14 and 3.6.x < 3.6.11 that is caused by Firefox not properly supporting calls with no arguments to window.__lookupGetter__. Such calls result in the use of a dangling pointer, which can lead to arbitrary code execution.
Strike Mozilla Firefox LookupUCProperty Memory Corruption	CWE: 119 CVE: 2007-2867 BID: 24242	This strike exploits a bug in Mozilla Firefox when referencing javascript objects whose internal proto attribute has been set to null.
Strike Mozilla Firefox Missing Frame Element Memory Corruption	CWE: 119 CVE: 2007-2867 BID: 24242	This strike exploits a bug in Mozilla Firefox when handling HTML documents with an IFRAME element that is deleted and then readded.
Strike Mozilla Firefox moz-grid Modification Denial of Service	CVE: 2006-1738 BID: 17516	This strike exploits a denial of service vulnerability in Mozilla Firefox when displaying a page that modifies the -moz-grid display style.

Name	References	Description
Strike Firefox 3.6.16 Object mChannel Use After Free	CWE: 399 CVE: 2011-0065	This strike triggers a vulnerability in Firefox 3.6.16 that is caused by the object mChannel getting freed and then subsequently used. Successful exploitation could lead to code execution.
Strike Mozilla Firefox onUnload() Memory Corruption	CVE: 2007-1092 BID: 22679	This strike exploits a memory corruption vulnerability in Mozilla Firefox when handling onUnload() events.
Strike Firefox Plugin Finder Javascript Injection Variant 1	BID: 13228 CVE: 2005-0752	This exploits a vulnerability that allows a 'javascript:' URL inside the 'pluginspage' attribute inside the HTML tag of a missing plugin.
Strike Firefox Plugin Finder Javascript Injection Variant 2	BID: 13228 CVE: 2005-0752	This exploits a vulnerability that allows a 'javascript:' URL inside the 'pluginspage' attribute inside the HTML tag of a missing plugin.
Strike Mozilla Firefox QueryInterface() Arbitrary Code Execution (Linux)	BID: 16476 CVE: 2006-0295	This strike exploits a code execution vulnerability in the Mozilla Firefox browser (targeting Linux).
Strike Mozilla Firefox QueryInterface() Arbitrary Code Execution (OS X)	BID: 16476 CVE: 2006-0295	This strike exploits a code execution vulnerability in Mozilla Firefox browser (targeting Mac OS X).
Strike Mozilla Firefox Style Engine Position Change Memory Corruption	CVE: 2006-0294 BID: 16476	This strike exploits a memory corruption vulnerability in Mozilla Firefox that occurs when a style element is changed from position:relative to position:static.
Strike Mozilla Firefox clipPath SVG stroke-width Memory Corruption	CWE: 119 CVE: 2007-0776 BID: 22964	This strike exploits a memory corruption vulnerability in Mozilla Firefox when rendering SVG documents with a large stroke-width xml property.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Mozilla Firefox SVG Processing Memory Corruption	CWE: 94  CVE: 2006-6504  BID: 21668	This strike exploits a memory corruption vulnerability in Mozilla Firefox when handling SVG documents in which child nodes are moved into the DOM tree using javascript.
Strike Mozilla Firefox SVG pathSegList.getItem Negative Argument Memory Corruption	CWE: 119  CVE: 2007-2867  BID: 24242	This strike exploits a bug in Mozilla Firefox when passing a negative argument to the pathSeglist.getItem() SVG method.
Strike Mozilla Firefox SVGZoom Memory Corruption	CWE: 119  CVE: 2007-2867  BID: 24242	This strike exploits a bug in Mozilla Firefox when changing the scaling factor on an SVG object that has been removed from the document.
Strike Mozilla Firefox TR Element Display=Inherit Memory Corruption	CWE: 119  CVE: 2007-2867  BID: 24242	This strike exploits a bug in Mozilla Firefox when dynamically inserting elements into a table with a TR tag with a crafted style attribute.
Strike Firefox Protocol Handler Code Execution Variant 1	BID: 25053  CVE: 2007-3845	This strike generates an HTML page containing malicious hyperlinks. If Internet Explorer 7 has been installed, these URIs will cause Firefox 2.0.0.5 to execute arbitrary commands
Strike Firefox Protocol Handler Code Execution Variant 2	BID: 25053  CVE: 2007-3845	This strike generates an HTML page containing malicious hyperlinks. If Internet Explorer 7 has been installed, these URIs will cause Firefox 2.0.0.5 to execute arbitrary commands
Strike Firefox Protocol Handler Code Execution Variant 3	BID: 25053  CVE: 2007-3845	This strike generates an HTML page containing malicious hyperlinks. If Internet Explorer 7 has been installed, these URIs will cause Firefox 2.0.0.5 to execute arbitrary commands

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Firefox Protocol Handler Code Execution Variant 4	BID: 25053 CVE: 2007-3845	This strike generates an HTML page containing malicious hyperlinks. If Internet Explorer 7 has been installed, these URIs will cause Firefox 2.0.0.5 to execute arbitrary commands
Strike Firefox URL Spoofing	CWE: 264 CVE: 2010-1206	When a new tab or window is opened in Firefox, the new url is put automatically into the address bar. An attacker can leverage this by opening a new window/tab with a url of his choosing and then calling window.stop(), which stops the new page from loading the content. Since the content from the url was never loaded, the new window document is still the about:blank document, which is considered to have the same origin as the parent window. This means that the parent window can access and manipulate the contents of the child window, which lets an attacker spoof a url of his choice.
Strike Firefox wyciwyg --Cache Manipulation Flaw (Defacing)	CWE: 200 CVE: 2007-3656 BID: 24831	This strike uses a flaw in the wyciwyg:// protocol of Firefox in conjunction with a 302 redirect to display modified cache content for any domain
Strike Firefox wyciwyg --Cache Manipulation Flaw (XSS)	CWE: 200 CVE: 2007-3656 BID: 24831	This strike uses a flaw in the wyciwyg:// protocol of Firefox in conjunction with a 302 redirect to display modified cache content for any domain
Strike Firefox XSLT Memory Corruption PoC	BID: 34235 CWE: 399 CVE: 2009-1169	This strike causes memory corruption in Firefox. This is a slightly different case than the one on Milworm. EIP should be invalid when the bug triggers.
Strike Firefox XSS Code Injection (FFRC)	BID: 13544 CVE: 2005-1477	This strike exploits a flaw in Firefox that results in execution of arbitrary code.
Strike Firefox XSS Code Injection (Generic)	BID: 13544 CVE: 2005-1477	This strike exploits a flaw in Firefox that results in execution of arbitrary code.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Mozilla Firefox XUL menupopup.menu Null Pointer Dereference	CVE: 2007-0775 BID: 22694	This strike exploits a null pointer dereference bug in Mozilla Firefox when parsing XUL XML files with a null menupopup.menu.
Strike Mozilla Firefox XUL Tree Node Removal	CVE: 2007-0775 BID: 22964	This strike exploits a memory corruption vulnerability in Mozilla Firefox when rendering XUL documents that programmaticaly modify the subelements of a tree node.
Strike Mozilla Firefox xulCommandDispatcher Deleted Object Memory Corruption	CWE: 119 CVE: 2007-2867 BID: 24242	This strike exploits a bug in Mozilla Firefox when handling XUL documents that reference deleted objects when calling xulCommandDispatcher functions.
Strike Adobe Flash 10 Corrupted SWF File		This strike exploits a flaw in Adobe Flash 10 that causes Internet Explorer 6/7/8 to crash while attempting to load a corrupted .swf file.
Strike Adobe Flash 9-10 ASnative(15,0) NULL Pointer Dereference		This strike exploits a NULL pointer dereference in the Adobe Flash browser plugin. This flaw is triggered when the ASnative method is used to call function 15-0 with a string as the first parameter.
Strike Adobe Flash 9-10 ASnative(301,1) NULL Pointer Dereference		This strike exploits a NULL pointer dereference in the Adobe Flash browser plugin. This flaw is triggered when the ASnative method is used to call function 301-1 with less than two parameters.
Strike Adobe Flash AVM Bytecode Verification Vulnerability	CVE: 2011-0609 BID: 46860	This strike exploits a vulnerability in Adobe Flash Player that can lead to remote code execution.
Strike Adobe Flash Player FLV Long String Buffer Overflow	CWE: 189 CVE: 2007-3456 BID: 24856	This strike exploits a buffer overflow in the Adobe Flash Player.
Strike Adobe Flash MP4 Memory Corruption	CWE: 119 CVE: 2012-0754 BID: 52034	This strike exploits a memory corruption vulnerability in Adobe Flash player, in the way it incorrectly validates the user supplied lengh of an MP4 file.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Adobe Flash 9-10 System.Product.launch() Command Execution	BID: 32896 CWE: 94 CVE: 2008-5499	This strike exploits a command execution flaw in Adobe Flash Player for Linux. Versions of Flash 10 below 10.0.12.36 and Flash 9 below 9.0.151.0 are vulnerable. This flaw can be used to execute system commands as the user running Flash.
Strike Flashchat aedating4CMS.php dir[inc] Parameter PHP File Include Variant 1	CWE: 94 CVE: 2006-4583 BID: 19826	This strike exploits a PHP include flaw in the Flashchat web application.
Strike Flashchat aedating4CMS.php dir[inc] Parameter PHP File Include Variant 2	CWE: 94 CVE: 2006-4583 BID: 19826	This strike exploits a PHP include flaw in the Flashchat web application.
Strike Flashchat aedating4CMS.php dir[inc] Parameter PHP File Include Variant 3	CWE: 94 CVE: 2006-4583 BID: 19826	This strike exploits a PHP include flaw in the Flashchat web application.
Strike FlashGameScript index.php func Parameter PHP File Include	BID: 22646 CWE: 94 CVE: 2007-1078	This strike exploits a PHP include flaw in FlashGameScript, an arcade website script.
Strike FlexBB index.php flexbb_lang_id Cookie SQL Injection	BID: 23161 CVE: 2007-1729	This strike exploits an SQL injection vulnerability in an unchecked cookie value in FlexBB
Strike Microsoft IIS Form_JScript.asp XSS		This strike attempts to access a sample script included with IIS 4.0 that is vulnerable to cross-site scripting (XSS).
Strike Formbook Oct 2021 Campaign - Command and Control		This strike simulates the 'Formbook Oct 2021 Campaign - Formbook Command and Control' traffic that occurs after executing the Formbook malware.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Forum Livre busca2.asp palavra Parameter HTTP Post Cross Site Scripting	CVE: 2007-0589  BID: 22246	This strike exploits a cross site scripting vulnerability in the Forum Livre web application.
Strike Free File Hosting forgot_pass.php AD_BODY TEMP Parameter PHP File Include	BID: 20781  CWE: 94  CVE: 2006-5762	This strike exploits a PHP include flaw in Free File Hosting versions prior to 1.1.
Strike Microsoft FrontPage DOS Device Name Crash Variant 1	BID: 1608  CVE: 2000-0709  CVE: 2000-0710	This strike attempts to crash the remote FrontPage enabled web server by requesting a DOS device name through the SHTML component.
Strike Microsoft FrontPage DOS Device Name Crash Variant 2	BID: 1608  CVE: 2000-0709  CVE: 2000-0710	This strike attempts to crash the remote FrontPage enabled web server by requesting a DOS device name through the SHTML component.
Strike Microsoft FrontPage DOS Device Name Crash Variant 3	BID: 1608  CVE: 2000-0709  CVE: 2000-0710	This strike attempts to crash the remote FrontPage enabled web server by requesting a DOS device name through the SHTML component.
Strike Microsoft FrontPage DOS Device Name Crash Variant 4	BID: 1608  CVE: 2000-0709  CVE: 2000-0710	This strike attempts to crash the remote FrontPage enabled web server by requesting a DOS device name through the SHTML component.
Strike Exodesk PHP Desk faq.php id Parameter SQL Injection (FullAspSite)	CVE: 2007-0678  BID: 22347	This strike exploits a SQL injection vulnerability in the Exodesk PHP Desk web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike GDIPPlus JPEG Processing Buffer Overrun - HTTP File Download	BID: 11173  CVE: 2004-0200	This strike exploits a vulnerability in the processing of JPEG images in multiple Microsoft products based on the GDIPPlus image library. This strike simulates downloading a JPEG via HTTP.
Strike GestArt aide.php3 aide Parameter PHP File Include	BID: 20750  CWE: 94  CVE: 2006-5612	This strike exploits a remote file include vulnerability in GestArt
Strike GitList Unauthenticated Remote Command Execution	EXPLOITDB : 44548	This strike exploits a remote command execution vulnerability in GitList. The vulnerability is due to improper sanitization of user-controlled values passed in search queries. By exploiting this vulnerability, a remote, unauthenticated attacker can execute arbitrary operating system commands on the target server.
Strike Google Chrome v8 Object.seal Map Transitions Type Confusion	GOOGLE: 1923	This strike exploits a vulnerability in Google Chrome. Specifically the vulnerability lies with how the v8 Javascript engine handles Object.seal/freeze on maps and element storage of objects, and how incorrect map transitions are followed by v8 without properly updating the element backing store. This can cause a denial of service condition in the browser but also leads to remote code execution.
Strike Google Chrome Javascript V8 Engine Integer Overflow		There are several integer overflow vulnerabilities in various functions in Google Chrome. One of the ways to access these functions is by concatenating large arrays. By doing this, an attacker can choose the amount by which to overflow an integer, which may lead to a stack overflow and arbitrary code execution.
Strike GrapAgenda index.php page Parameter PHP File Include	CVE: 2006-4610  BID: 19857	This strike exploits a PHP include flaw in GrapAgenda web application.
Strike Hancitor Malware April 2020 Campaign Command and Control Data Exfiltration		This strike simulates the Hancitor Malware April 2020 Campaign Command and Control traffic that occurs after installing the 'VBS' module with the following steps 1. Client sends HTTP GET request - Server replies with the IP address of client 2. Host/OS-Version data is exfiltrated via HTTP GET request - Server replies with the encoding algorithm works like Base64Encode(XOR(URL_List)) that are used for the next phase of the attack where requests are made 3. Client sends HTTP POST request - Server replies with unknown binary data
Strike HP Intelligent Management Center Unauthenticated File Retrieval		This strike exploits a directory traversal vulnerability presents in the HP Intelligent Management Center. The vulnerability is due to insufficient validation of traverse directory requests. The remote attacker may disclosure the information in the target system.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike HP OpenView Network Node Manager AcceptLang Buffer Overflow	CWE: 119 CVE: 2009-0921 BID: 34135	This strike sends a malicious cookie value that will trigger a buffer overflow condition on vulnerable installations of HP OpenView Network Node Manager web application.
Strike HP OpenView Network Node Manager OvOsLocale Buffer Overflow	CWE: 119 CVE: 2009-0920 BID: 34294	This strike sends a malicious cookie value that will trigger a buffer overflow condition on vulnerable installations of HP OpenView Network Node Manager web application.
Strike HP Universal CMDB Server Credential Code Execution		This audit exploits a default credentials vulnerability in HP Universal CMDB server. Attackers can use this vulnerability to bypass the authentication on the target system.
Strike Headline Portal Engine page.newnews.show.php3 HPEinc Parameter PHP File Include	BID: 19663	This strike exploits a PHP include flaw in the Headline Portal Engine web application. An attacker could exploit this vulnerability to execute arbitrary server-side script code.
Strike Headline Portal Engine thememaker.php3 HPEinc Parameter PHP File Include Variant 2	BID: 19663	This strike exploits a PHP include flaw in the Headline Portal Engine web application. An attacker could exploit this vulnerability to execute arbitrary server-side script code.
Strike Microsoft IIS HTR Source Fragment Disclosure	CVE: 2001-0004 BID: 2313	This strike attempts to retrieve the source code of 'global.asa' by exploiting a parsing flaw in the HTR ISAPI filter.
Strike IBiz EBanking Integrator ActiveX WriteOFXDataFile Method Arbitrary File Write	BID: 28700 CVE: 2008-1725	This strike exploits an arbitrary file write bug in the IBiz EBanking ActiveX control when calling the WriteOFXDataFile method.
Strike IBM Lotus Domino HPRAgentName buffer overflow		This strike exploits an IBM Lotus Domino buffer overflow vulnerability. This vulnerability is due to bad input check the boundary of the parameter. Remote attackers may do arbitrary code execution on the target system.

Name	References	Description
Strike IBM Lotus Domino Web Access ActiveX Control Buffer Overflow	CWE: 119 CVE: 2007-4474 BID: 26972	There exists a stack-based buffer overflow in the IBM Lotus Domino Web Access 7.x ActiveX control in dwa7W.dll which potentially allows remote attackers to execute arbitrary code via an overly long string supplied as the parameter ServerName of General_ServerName property which is processed by the affected method InstallBrowserHelperDll() which has improper bounds checking. This strike delivers a payload via an html page that is consistent with triggering the vulnerable conditions of this ActiveX control method buffer overflow flaw.
Strike IBM Lotus Sametime StMux.exe Buffer Overflow	CWE: 119 CVE: 2008-2499 BID: 29328	This strike triggers a stack buffer overflow in IBM Lotus Sametime Server (StMux.exe) by doing a POST request with an overly long path.
Strike IBM WebSphere Application Server Cross-Site Scripting	BID: 34001 CWE: 79 CVE: 2009-0855 CVE: 2009-0856	This strike exploits an XSS attack on an IBM WebSphere Application Server.
Strike IcedID Dec 2020 Campaign - IcedID Loader Command and Control		This strike simulates the 'IcedID Dec 2020 Campaign - IcedID Loader Command and Control' traffic that occurs after executing the IcedID Loader malware.
Strike ICloudCenter ICJobSite 1.1 index.php pid Parameter SQL Injection Vulnerability	CWE: 89 CVE: 2011-1557 BID: 47100	This strike exploits a SQL injection flaw in ICloudCenter's ICJobSite 1.1 web application.
Strike Microsoft IIS IDA Path Disclosure	BID: 1065 CVE: 2000-0071	This strike attempts to discover the physical path of the web root by requesting a non-existent IDA file.
Strike IDAutomation Aztec SaveBarcode ActiveX Arbitrary File Write	BID: 29204 CWE: 20 CVE: 2008-2283	This strike exploits an arbitrary file write vulnerability in the IDAutomation Aztec ActiveX control.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike IDAutomation Aztec SaveEnhWMF ActiveX Arbitrary File Write	BID: 29204 CWE: 20 CVE: 2008-2283	This strike exploits an arbitrary file write vulnerability in the IDAutomation Aztec ActiveX control.
Strike IDAutomation DataMatrix SaveBarcode ActiveX Arbitrary File Write	BID: 29204 CWE: 20 CVE: 2008-2283	This strike exploits an arbitrary file write vulnerability in the IDAutomation Aztec ActiveX control.
Strike IDAutomation DataMatrix SaveEnhWMF ActiveX Arbitrary File Write	BID: 29204 CWE: 20 CVE: 2008-2283	This strike exploits an arbitrary file write vulnerability in the IDAutomation Aztec ActiveX control.
Strike IDAutomation Linear SaveBarcode ActiveX Arbitrary File Write	BID: 29204 CWE: 20 CVE: 2008-2283	This strike exploits an arbitrary file write vulnerability in the IDAutomation Aztec ActiveX control.
Strike IDAutomation Linear SaveEnhWMF ActiveX Arbitrary File Write	BID: 29204 CWE: 20 CVE: 2008-2283	This strike exploits an arbitrary file write vulnerability in the IDAutomation Aztec ActiveX control.
Strike IDAutomation PDF SaveBarcode ActiveX Arbitrary File Write		This strike exploits an arbitrary file write vulnerability in the IDAutomation Aztec ActiveX control.
Strike Microsoft IIS IDQ Path Disclosure	BID: 1065 CVE: 2000-0071	This strike attempts to discover the physical path of the web root by requesting a non-existent IDQ file.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike MSIE7 ActiveX Control BrowseDialog Denial of Service	BID: 22110 CVE: 2007-0371	This strike causes a denial of service in Microsoft Internet Explorer 7 by exploiting a bug in the 'BrowseDialog' ActiveX control.
Strike IE8 CSS Import Remote Code Execution Vulnerability	CWE: 399 CVE: 2010-3971 BID: 45246	This strike exploits a vulnerability in Internet Explorer 8's handling of various @import css declarations.
Strike Microsoft Internet Explorer VML Use After Free CVE 2012-0172	CWE: 94 CVE: 2012-0172	This strike exploits a user after free vulnerability in Microsoft Internet Explorer. This can be seen when VML is used in an HTML body element and script code is used in the style attribute of the body element to clear the document. A use after free condition is observed if the elements are cleared or destroyed and referenced later.
Strike Microsoft Internet Explorer Uninitialized Object Memory Corruption	CWE: 20 CVE: 2011-1995	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer. It is due to uninitialized object(ActiveX controls)access where arbitrary attributes can be set, and then along with their child attributes can be accessed. This can possibly allow remote code execution as well as cause a termination of the application.
Strike Internet Explorer ADODB.Recordset.Filter DoS	BID: 18773 CVE: 2006-3354	This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the ADODB.Recordset COM object.
Strike Internet Explorer Applet File Path DoS	BID: 15208	This strike exploits a denial of service flaw in the Internet Explorer web browser.
Strike Internet Explorer NMSAASFSourceMediaDescription.value DoS	BID: 19114 CVE: 2006-3897	This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the NMSAASFSourceMediaDescription COM object.
Strike Internet Explorer AxDebugger.Document DoS		This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the AxDebugger.Document COM object.
Strike Internet Explorer 7.0 Beta 2 BG SOUND DoS	CVE: 2006-0544 BID: 22621	This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the BG SOUND element with a long local file name specified as the source.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike CapiCom.Utilities ActiveX GetRandom Integer Overflow Denial of Service		This strike causes a denial of service in Microsoft's CapiCom.Utilities ActiveX Control by exploiting an integer overflow in the 'GetRandom' function.
Strike Microsoft Internet Explorer circular reference	CWE: 399 CVE: 2009-3674	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer. It exists due to improper handling of script-modified DOM structures when an HTML document is being parsed. When a circular reference between two DOM objects is created, it is not validated after the objects are later removed from the main markup.
Strike Internet Explorer Comctl32.dll Heap Overflow	CWE: 119 CVE: 2010-2746 BID: 43717	This strike exploits a vulnerability in comctl32.dll by delivering an invalid svg to the victim.
Strike Internet Explorer createTextRange() Code Execution Variant 1	BID: 17196 CWE: 94 CVE: 2006-1359	This strike exploits a code execution vulnerability in Internet Explorer.
Strike Internet Explorer createTextRange() Code Execution Variant 2	BID: 17196 CWE: 94 CVE: 2006-1359	This strike exploits a code execution vulnerability in Internet Explorer.
Strike Internet Explorer createTextRange() Code Execution Variant 3	BID: 17196 CWE: 94 CVE: 2006-1359	This strike exploits a code execution vulnerability in Internet Explorer.
Strike Internet Explorer createTextRange() Code Execution Variant 4	BID: 17196 CWE: 94 CVE: 2006-1359	This strike exploits a code execution vulnerability in Internet Explorer.

Name	References	Description
Strike Internet Explorer createTextRange() Code Execution Variant 5	BID: 17196  CWE: 94  CVE: 2006-1359	This strike exploits a code execution vulnerability in Internet Explorer.
Strike Internet Explorer createTextRange() Code Execution Variant 6	BID: 17196  CWE: 94  CVE: 2006-1359	This strike exploits a code execution vulnerability in Internet Explorer.
Strike Microsoft IE CSS Memory Corruption	CVE: 2004-0842  BID: 10816	This strike exploits a vulnerability in Internet Explorer that causes a heap overflow due to an unterminated multi-line comment in a style tag.
Strike Internet Explorer DirectAnimation.DA UserData.Data DoS	BID: 18902  CVE: 2006-3513	This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the DirectAnimation.DAUserData COM object.
Strike Internet Explorer DirectAnimation.StructuredGraphicsControl.SourceURL DoS	BID: 18855  CVE: 2006-3427	This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the DirectAnimation.StructuredGraphicsControl COM object.
Strike Microsoft Internet Explorer use after free Null reference	CWE: 20  CVE: 2011-1997  BID: 49962	This strike exploits a user after free vulnerability in Microsoft Internet Explorer. When an attributes element is set to Null and cleared by the GarbageCollector, it can still be referenced later allowing for the corruption of memory.
Strike Internet Explorer File Upload Keystroke Hijack	CWE: 200  CVE: 2006-2900  BID: 18308	This strike exploits a user interface misdirection vulnerability in Microsoft Internet Explorer. Due to lax control of the input text field for the file upload widget, a malicious website may redirect keystrokes intended for one element of a frame to the file upload widget. This technique can be used to cause a victim to unknowingly upload a local file to the remote web site.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer FTP Web View XSS	CVE: 2002-2062 BID: 4954	This strike exploits a cross site scripting vulnerability in Microsoft Internet Explorer when Internet Explorer is configured to enable folder view for web sites and allows web content in folders.
Strike Internet Explorer HtmlDlgSafeHelper.HtmlDlgSafeHelper.BlockFormats DoS		This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the HtmlDlgSafeHelper.HtmlDlgSafeHelper COM object.
Strike Internet Explorer iepeers.dll Use-After-Free Vulnerability	CWE: 399 CVE: 2010-0806 BID: 38615	This strike exploits a use after free vulnerability that is present inside Microsoft IE, which gets triggered through actions that are taken by an embedded object. Remote attacker can use this vulnerability to do code execution on the target system.
Strike Internet Explorer IFRAME Overflow	CVE: 2004-1050 BID: 11515	This strike exploits a buffer overflow flaw in the handling of IFRAME NAME properties in Microsoft Internet Explorer.
Strike Internet Explorer Internet.PopupMenu .RemoveItem DoS		This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the Internet.PopupMenu COM object.
Strike Microsoft Internet Explorer Javascript For Loop Denial of Service	CVE: 2007-0811 BID: 22408	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when processing Javascript for-loops.
Strike IE Long Hostname Memory Corruption	CVE: 2005-0554 BID: 13123	This strike exploits a denial of service flaw in Microsoft Internet Explorer when handling long hostnames.
Strike Internet Explorer mdsauth.dll Arbitrary File Overwrite	CVE: 2007-2221 BID: 23827	This strike exploits an arbitrary remote file overwrite bug in Internet Explorer when browsing a page that contains a vulnerable COM object.
Strike Internet Explorer Microsoft.ISCatAdm DoS	CVE: 2006-4495 BID: 19636	This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the Microsoft.ISCatAdm COM object.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer Mouse Drag Hijack	CVE: 2004-0841 BID: 10690	This strike exploits a flaw in Internet Explorer that allows Javascript calls to hijack mouse events.
Strike Internet Explorer JPEG Processing DoS (CMP)	CVE: 2005-2308 BID: 14284	This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through a malformed JPEG image.
Strike Internet Explorer JPEG Processing DoS (MOV)	BID: 14282 CVE: 2005-2308	This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through a malformed JPEG image.
Strike Internet Explorer JPEG Processing DoS (OOM)	BID: 14285 CVE: 2005-2308	This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through a malformed JPEG image.
Strike Internet Explorer EMF File Rendering Denial of Service (HTTP)	CWE: 399 CVE: 2005-0803 BID: 12834	This strike exploits a denial of service flaw in Microsoft Windows. This flaw is triggered through a malformed Windows EMF Metafile. This strike simulates downloading an EMF file via HTTP.
Strike Internet Explorer WMF File Rendering Denial of Service (HTTP)	CVE: 2005-2124 BID: 15356	This strike exploits a denial of service flaw in Microsoft Windows. This flaw is triggered through a malformed Windows WMF Metafile. This strike simulates downloading an WMF file via HTTP.
Strike Microsoft Internet Explorer Corrupted True Type Font	CVE: 2011-3402 BID: 50462	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when using a corrupted true type font. duku uses this for its attack.
Strike Microsoft Internet Explorer Time Behavior Use After Free	CWE: 94 CVE: 2011-3397 BID: 50970	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when using the deprecated time behavior.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer winhlp32.exe MsgBox() Remote Code Execution Vulnerability	CWE: 94 CVE: 2010-0483 BID: 38463	This strike exploits the way VBScript interacts with Windows Help files when using Internet Explorer. If an attacker can trick the user into pressing F1 after a dialog is displayed, he/she can run arbitrary code on the user's machine.
Strike Internet Explorer MSHTML Parsing DoS	BID: 16079	This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through a specific malformed block of HTML code.
Strike Internet Explorer NMSA.MediaDescription.dispvalue DoS	BID: 19114 CVE: 2006-3897	This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the NMSA.MediaDescription COM object.
Strike Microsoft Internet Explorer Temporary Internet Files Folder Access	CVE: 2002-1188 BID: 6217	This strike exploits an vulnerability in Microsoft Internet Explorer that allows temporary internet files to be referenced in the local zone.
Strike Microsoft Internet Explorer use-after-free onreadystatechange	CWE: 399 CVE: 2010-0491 BID: 39027	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer. It exists due to a use-after-free error when parsing HTML with the onreadystatechange event.
Strike Use After Free CMarkup Vulnerability in Microsoft Internet Explorer	CWE: 119 CVE: 2014-4085 BID: 69589	This strike exploits a use after free vulnerability inside Microsoft Internet Explorer. This vulnerability is due to an error that occurs when handling CMarkup objects. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike Microsoft Internet Explorer Option Element Memory Corruption	CWE: 20 CVE: 2011-1996 BID: 49961	This strike exploits the way Microsoft Internet Explorer handles the Option Element within an Option cache. Using the innerHTML and innerText properties will delete the DOM subtree w/o rebuilding the Options cache. If they are reset pre-existing options will be referenced even after deleted.
Strike Internet Explorer OutlookExpress.AddressBook DoS	CWE: 119 CVE: 2005-4840	This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the OutlookExpress.AddressBook COM object.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer Outlook Express Address Book ActiveX DoS	CWE: 119 CVE: 2005-4840	This strike exploits crashes Internet Explorer by loading the Outlook Express address book as an ActiveX object
Strike Microsoft Internet Explorer Print Table of Links Local Zone XSS		This strike exploits a local-zone cross-site scripting vulnerability in Microsoft Internet Explorer when using the "print table of links" functionality.
Strike Internet Explorer RDS.DataControl.URL DoS	BID: 18900 CVE: 2006-3510	This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the RDS.DataControl COM object.
Strike Remote Desktop Connection ActiveX Control Heap Overflow Vulnerability	CWE: 119 CVE: 2009-1929 BID: 35973	This strike exploits a vulnerability in the way the Remote Desktop ActiveX Control validates input from functions available for scripting, resulting in a heap overflow and possibly arbitrary code execution.
Strike Microsoft Internet Explorer Select Element Memory Corruption	CWE: 20 CVE: 2011-1999 BID: 49964	This strike exploits the way Microsoft Internet Explorer handles the Select Element. If a OBefore parameter in the add method is negative, it doesn't validate the number, and instead uses it directly as an index.
Strike Internet Explorer Sysmon DoS		This strike exploits a denial of service flaw in the Internet Explorer web browser. This flaw is triggered through the Sysmon COM object.
Strike Internet Explorer TSUserEX.DLL ActiveX	CVE: 2006-4219 BID: 19570	This strike instantiates TSUserEX.DLL which causes IE 6 SP1 on Windows 2003 Server CN to crash.
Strike Internet Explorer VML Fill Method Buffer Overflow Variant 1	CWE: 119 CVE: 2006-4868 BID: 20096	This strike exploits a code execution vulnerability in Internet Explorer.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer VML Fill Method Buffer Overflow Variant 2	CWE: 119 CVE: 2006-4868 BID: 20096	This strike exploits a code execution vulnerability in Internet Explorer.
Strike Internet Explorer VML Fill Method Buffer Overflow Variant 3	CWE: 119 CVE: 2006-4868 BID: 20096	This strike exploits a code execution vulnerability in Internet Explorer.
Strike Internet Explorer VML Fill Method Buffer Overflow Variant 4	CWE: 119 CVE: 2006-4868 BID: 20096	This strike exploits a code execution vulnerability in Internet Explorer.
Strike Internet Explorer VML Fill Method Buffer Overflow Variant 5	CWE: 119 CVE: 2006-4868 BID: 20096	This strike exploits a code execution vulnerability in Internet Explorer.
Strike Internet Explorer VML Fill Method Buffer Overflow Variant 6	CWE: 119 CVE: 2006-4868 BID: 20096	This strike exploits a code execution vulnerability in Internet Explorer.
Strike Internet Explorer VML Fill Method Buffer Overflow Variant 7	CWE: 119 CVE: 2006-4868 BID: 20096	This strike exploits a code execution vulnerability in Internet Explorer.
Strike Internet Explorer VML Fill Method Buffer Overflow Variant 8	CWE: 119 CVE: 2006-4868 BID: 20096	This strike exploits a code execution vulnerability in Internet Explorer.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer VML Fill Method Buffer Overflow Variant 9	CWE: 119 CVE: 2006-4868 BID: 20096	This strike exploits a code execution vulnerability in Internet Explorer.
Strike Microsoft Windows WinHlp Item Buffer Overflow	CVE: 2002-0823 BID: 4857	This strike exploits Microsoft Internet Explorer using a buffer overflow vulnerability in the WinHlp ActiveX control.
Strike Internet Explorer WMF CreateBrushIndirect () DoS	CVE: 2006-4071 BID: 19365	This strike exploits a denial of service flaw in the GDI32 CreateBrushIndirect() function using Internet Explorer and the WMF file format.
Strike Internet Explorer 8 CSS import toStaticHTML XSS filter bypass	CWE: 79 CVE: 2010-3324 BID: 42467	This strike bypasses the anti-XSS functionality of the toStaticMethod in Internet Explorer 8.
Strike Ignite Realtime Openfire Server Cross-Site Scripting (XSS)		This strike exploits a cross-site scripting vulnerability in Ignite Realtime Openfire Server. The vulnerability is due to improper validation of HTTP request hostname parameter. By exploiting this vulnerability an attacker could execute arbitrary scripts on the target machine.
Strike Microsoft IIS 5.1 Alternate Data Stream Authentication Bypass	BID: 41314 CWE: 287 CVE: 2010-2731	This strike exploits a vulnerability in Microsoft IIS 5.1 that allows a user to bypass directory access restrictions. If a user appends "::\$i30:\$INDEX_ALLOCATION" to the directory name in a url, he is granted access.
Strike Microsoft IIS idq.dll IDA-IDQ ISAPI Overflow Variant 1	CVE: 2001-0500 BID: 2880	This strike exploits a buffer overflow vulnerability in Microsoft IIS idq.dll.
Strike Microsoft IIS idq.dll IDA-IDQ ISAPI Overflow Variant 2	CVE: 2001-0500 BID: 2880	This strike exploits a buffer overflow vulnerability in Microsoft IIS idq.dll.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike IIS Long URL QoS Denial of Service	CWE: 399 CVE: 2011-1965 BID: 48990	This strike exploits a denial of service bug in the URL based QoS processing of a long URI in the IIS Web Server.
Strike iLife Photocast XML Title Format String Variant 1	CWE: 134 CVE: 2007-0051 BID: 21871	This strike exploits a format string vulnerability in Apple iLife. The flaw lies in the parsing of the title field of an iPhoto RSS feed. By convincing a user to subscribe to a malicious RSS Feed, an attacker could remotely execute arbitrary code. This strike emulates the original PoC.
Strike InterAKT Online MX Shop index.php idp Parameter SQL Injection	BID: 14876 CVE: 2005-3004	This strike exploits a SQL injection vulnerability in InterAKT Online MX Shop
Strike InterAKT Online MX Shop index.php id_ctg Parameter SQL Injection	BID: 14876 CVE: 2005-3004	This strike exploits a SQL injection vulnerability in InterAKT Online MX Shop
Strike InterAKT Online MX Shop index.php id_prd Parameter SQL Injection	BID: 14876 CVE: 2005-3004	This strike exploits a SQL injection vulnerability in InterAKT Online MX Shop
Strike inTouch index.php user Parameter SQL Injection	CVE: 2006-0088 BID: 16110	This strike exploits a SQL injection flaw in the inTouch Web Application.
Strike Invisionix Roaming System pageheaderdefault.inc.php _sysSessionPath Parameter PHP File Include	CVE: 2006-4237 BID: 19567	This strike exploits a PHP remote file include flaw in Invisionix Roaming System Remote.
Strike IPSwitch WhatsUp Gold maincfgret.cgi instancename Parameter Buffer Overflow	CVE: 2004-0798 BID: 11043	This strike exploits a buffer overflow in a CGI executable from the IPSwitch WhatsUp Gold network monitoring tool

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft IIS .htn ISAPI Chunked Encoding Overflow	CVE: 2002-0364  BID: 4855	This strike exploits a heap overflow in the HTR ISAPI filter of Microsoft IIS versions 4.0 and 5.0.
Strike Microsoft IIS 5.0 ISAPI .printer Extension Host Header Overflow Variant 2	CVE: 2001-0241  BID: 2674	This strike exploits a buffer overflow in the .printer ISAPI extension for Microsoft IIS 5.0 when handling long Host HTTP headers.
Strike ITunes ITMS Url Parsing Buffer Overflow	CWE: 119  CVE: 2009-0950  BID: 35157	This strike exploits a vulnerability in iTunes 8.1.x itms url parsing
Strike ITunes ITPC Url Parsing Buffer Overflow	CWE: 119  CVE: 2009-0950  BID: 35157	This strike exploits a vulnerability in iTunes 8.1.x itpc url parsing
Strike Oracle Java FileDialog.Show Heap Buffer Overflow	CVE: 2011-0802  BID: 48149	This strike triggers a heap-based buffer overflow in Oracle's Java interpreter by passing an overly long string to the FileDialog::setFile function.
Strike JBoss Application Server Java Unserialization	BID: 77539  CWE: 77  CVE: 2015-4852	This strike exploits a Java Unserialization vulnerability in JBoss application server. The vulnerability is due to unsafe unserialization of java objects, including from untrusted sources By enticing a user to visit a malicious web page, arbitrary command can be executed on the client system.
Strike Joomla! Component EkRishta 2.10 - username SQL Injection	EXPLOITDB : 44877	This strike exploits an Error-Based SQL injection vulnerability in Joomla! Component EkRishta 2.10. The vulnerability is caused by insufficient validation of user input on HTTP requests which are used to create SQL queries. Successful exploitation could allow an attacker to see the database information on the target server.
Strike Joomla 1.7.0 Request URI index.php XSS	CWE: 79  CVE: 2011-2710	This strike exploits a cross site scripting flaw in the Request URI method of the Joomla Content Management System.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Joomla Webring Component admin.webring.docs.php component_dir Parameter PHP File Include	CVE: 2006-4129 BID: 19492	This strike exploits a PHP include flaw in Joomla Content Management Application.
Strike Knusperleicht Shoutbox index.php sb_include_path Parameter PHP File Include	CVE: 2006-3989 BID: 19273	This strike exploits a PHP include flaw in the Knusperleicht Shoutbox web application.
Strike Konqueror FTP IFrame Null Pointer Dereference	CWE: 399 CVE: 2007-1308 BID: 22814	This strike causes a denial of service in Konqueror by accessing properties of an iframe with an FTP type src attribute
Strike Lazarus Jan 2022 Campaign - Malicious-Module Command and Control		This strike simulates the Command and Control traffic that occurs after executing the DLL embedded Malicious-Module.
Strike LBlog comments.asp id Parameter SQL Injection	CVE: 2006-4284 BID: 19607	This strike exploits a SQL injection flaw in the LBlog blogging web application to disclose information from the underlying database.
Strike libpng png_handle_sBIT() Local Overflow (HTTP)	BID: 10857 BID: 15495 CVE: 2004-0597	This strike exploits a vulnerability in the processing of PNG images by libpng. This strike simulates downloading a PNG via HTTP.
Strike phpBook index.php date Parameter PHP Code Execution	CVE: 2006-0206 BID: 16229	This strike exploits an arbitrary code execution flaw in the LightWeight Calendar web application.
Strike Linksys E Series ttcp_ip Remote Code Execution	EXPLOITDB : 31683	This strike exploits a remote code execution vulnerability on Linksys E Series Router. This vulnerability is due to improper handling of the parameter under "ttcp_ip" under http request. A remote unauthenticated attacker can exploit this vulnerability by sending crafted http requests to the target server. Successful exploitation results in remote code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Linksys WRH54G HTTP Management Interface DoS	CWE: 20 CVE: 2008-2636	The HTTP management interface of the Linksys WRH54G wireless router is vulnerable to a DoS attack when it receives a maliciously crafted url.
Strike Liquid XML Studio 2010 OpenFile() ActiveX Buffer Overflow		This strike exploits a buffer overflow vulnerability present in the OpenFile() method of the LtXmlComHelp8.dll ActiveX control included with Liquid XML Studio 2010.
Strike Liquid XML studio ActiveX openfile BO		This strike exploits buffer overflow vulnerability within a Liquid XML studio ActiveX. This vulnerability is due to lack of confirmation of filename length when handling the openfile function. Remote unauthenticated attackers could exploit this vulnerability to execute arbitrary code on the target system
Strike Lizard Cart CMS pages.php id Parameter SQL Injection	CVE: 2006-0087 BID: 16140	This strike exploits a SQL injection flaw in the Lizard Cart CMS web application.
Strike Lizard Cart CMS detail.php id Parameter SQL Injection	CVE: 2006-0087 BID: 16140	This strike exploits a SQL injection flaw in the Lizard Cart CMS web application.
Strike Microsoft Windows LoadImage API Overflow (HTTP)	BID: 12095 CVE: 2004-1049	This strike exploits a flaw in the parsing of images via LoadImage on Microsoft Windows. This strike simulates downloading a malicious .ani animated cursor from a web server.
Strike IBM Lotus Domino HTTP Header Accept-Language Buffer Overflow	CWE: 119 CVE: 2008-2240 BID: 29310	This strike exploits a buffer overflow flaw in the IBM Lotus Domino web server. If a specially formatted URI is requested in combination with an overly long Accept-Language value, the flaw will be triggered, possibly allowing an attacker to execute arbitrary code.
Strike IBM Lotus Domino HTTP Redirect Buffer Overflow	CVE: 2003-0178 BID: 6870	This strike exploits a buffer overflow flaw in the IBM Lotus Domino web server.
Strike IBM Lotus Domino Web Server Denial of Service	CVE: 2005-0986	This strike exploits a flaw in the IBM Lotus Domino web server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike IBM Lotus iNotes Buffer Overflow Vulnerability	CVE: 2003-0178 BID: 6871	This strike exploits a buffer overflow flaw in the IBM Lotus iNotes web server.
Strike Macromedia Coldfusion Remote SYSTEM Buffer Overflow (Filename)	CVE: 2002-1992 BID: 5121	This strike exploits a remote buffer overflow in the Macromedia Coldfusion 6.0 IIS ISAPI handler.
Strike Macromedia Shockwave swdir.dll ActiveX Control Remote Stack Overflow (Autostart)	CVE: 2007-1403 BID: 22842	This strike exploits a stack overflow in an ActiveX control in Macromedia Shockwave 10.1.4.20's swdir.dll to cause arbitrary code execution.
Strike Macromedia Shockwave swdir.dll ActiveX Control Remote Stack Overflow (BGColor)	CVE: 2007-1403 BID: 22842	This strike exploits a stack overflow in an ActiveX control in Macromedia Shockwave 10.1.4.20's swdir.dll to cause arbitrary code execution.
Strike Macromedia Shockwave swdir.dll ActiveX Control Remote Stack Overflow (Drawlogo)	CVE: 2007-1403 BID: 22842	This strike exploits a stack overflow in an ActiveX control in Macromedia Shockwave 10.1.4.20's swdir.dll to cause arbitrary code execution.
Strike Macromedia Shockwave swdir.dll ActiveX Control Remote Stack Overflow (Drawprogress)	CVE: 2007-1403 BID: 22842	This strike exploits a stack overflow in an ActiveX control in Macromedia Shockwave 10.1.4.20's swdir.dll to cause arbitrary code execution.
Strike Macromedia Shockwave swdir.dll ActiveX Control Remote Stack Overflow (Sound)	CVE: 2007-1403 BID: 22842	This strike exploits a stack overflow in an ActiveX control in Macromedia Shockwave 10.1.4.20's swdir.dll to cause arbitrary code execution.
Strike Macromedia Shockwave swdir.dll ActiveX Control Remote Stack Overflow (SRC)	CVE: 2007-1403 BID: 22842	This strike exploits a stack overflow in an ActiveX control in Macromedia Shockwave 10.1.4.20's swdir.dll to cause arbitrary code execution.
Strike Macromedia Shockwave SWDIR.SLL ActiveX Denial of Service (Autostart)	CVE: 2006-6885 BID: 22067	This strike exploits a Shockwave ActiveX plugin that is vulnerable to a denial of service.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Macromedia Shockwave SWDIR.SLL ActiveX Denial of Service (Bgcolor)	CVE: 2006-6885 BID: 22067	This strike exploits a Shockwave ActiveX plugin that is vulnerable to a denial of service.
Strike Macromedia Shockwave SWDIR.SLL ActiveX Denial of Service (DrawLogo)	CVE: 2006-6885 BID: 22067	This strike exploits a Shockwave ActiveX plugin that is vulnerable to a denial of service.
Strike Macromedia Shockwave SWDIR.SLL ActiveX Denial of Service (DrawProgress)	CVE: 2006-6885 BID: 22067	This strike exploits a Shockwave ActiveX plugin that is vulnerable to a denial of service.
Strike Macromedia Shockwave SWDIR.SLL ActiveX Denial of Service (Sound)	CVE: 2006-6885 BID: 22067	This strike exploits a Shockwave ActiveX plugin that is vulnerable to a denial of service.
Strike Macromedia Shockwave SWDIR.SLL ActiveX Denial of Service (SRC)	CVE: 2006-6885 BID: 22067	This strike exploits a Shockwave ActiveX plugin that is vulnerable to a denial of service.
Strike Macromedia Shockwave SWDIR.SLL ActiveX Denial of Service (SWURL)	CVE: 2006-6885 BID: 22067	This strike exploits a Shockwave ActiveX plugin that is vulnerable to a denial of service.
Strike MagnetoSoft DNS DNSLookupHostWithServer ActiveX Control Format String		This module exploits a format string flaw in the MagnetoSoft DNS DNSLookupHostWithServer ActiveX Control.
Strike MagnetoSoft ICMP AddDestinationEntry ActiveX Control Buffer Overflow		This module exploits a buffer overflow in the MagnetoSoft ICMP AddDestinationEntry ActiveX Control.
Strike MagnetoSoft NetResources NetConnectionEnum ActiveX Control Buffer Overflow		This module exploits a buffer overflow in the MagnetoSoft NetResources NetConnectionEnum ActiveX Control.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike MagnetoSoft NetResources NetSessionDel ActiveX Control Buffer Overflow		This module exploits a buffer overflow in the MagnetoSoft NetResources NetSessionDel ActiveX Control.
Strike MagnetoSoft SNTP SntpGetReply ActiveX Control Buffer Overflow		This module exploits a buffer overflow in the MagnetoSoft SNTP SntpGetReply ActiveX Control.
Strike Operation Quicksand Nov 2020 Campaign - Powershell Malware File Transfer	MD5: 2e7b4ae4b aa70458824 8b425b8e02 7bf  SHA1: 60b5b41bd5 98fd844630 fdf609539fc 854437392  SHA256: 8bbcd7013 e339cca41c f85a0788ef0 fc250b5451 5a038eff6d4 838a16be04 7d7	This strike simulates the download of the Powershell malware via an HTTP GET request.
Strike Mambo Gallery Manager help.mgm.php mosConfig_absolute_path Parameter PHP File Include	CWE: 94  CVE: 2006-3980  BID: 19224	This strike exploits a PHP include flaw in the Mambo Gallery Manager web application.
Strike Mambo VideoDB Component Module videodb.class.xml.php mosConfig_absolute_path Parameter PHP File Include	CVE: 2006-3736  BID: 19049	This strike exploits a PHP include flaw in the VideoDB component of the Mambo web application.
Strike Matanbuchus Jun 2022 Campaign - Cobalt Strike Beacons		This strike simulates the 'Matanbuchus Jun 2022 Campaign - Cobalt Strike Beacons' traffic that occurs once the Matanbuchus command and control traffic has been sent. This strike sends 2 HTTP GET requests to the command and control server to download Cobalt Strike beacons. The first request downloads a hexadecimal binary that gets converted to ASCII characters, and the second request downloads a dll.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike McAfee EPolicy Orchestrator Source Header Overflow	BID: 20288 CVE: 2006-5156	This strike exploits buffer overflow in the EPolicy Orchestrator HTTP service.
Strike McAfee Subscription Manager ActiveX vsprintf	BID: 19265 CWE: 119 CVE: 2006-3961	This strike exploits a printf-style flaw in the McAfee Subscription Manager ActiveX control
Strike Trojan.MDropper Word Document (http) Variant 1	BID: 18037 CVE: 2006-2492	The Trojan.MDropper malware abuses an arbitrary code execution flaw in Microsoft Office.
Strike Trojan.MDropper Word Document (http) Variant 2	BID: 18037 CVE: 2006-2492	The Trojan.MDropper malware abuses an arbitrary code execution flaw in Microsoft Office.
Strike ME Download System header.php Vb8878b936c2bd8a e0cab Parameter PHP File Include	CVE: 2006-4053 BID: 19336	This strike exploits a PHP include flaw in the ME Download System web application.
Strike MediaWiki index.php rs Cross-Site Scripting	BID: 21956 CVE: 2007-0177	This strike exploits a cross-site scripting vulnerability in the experimental AJAX functionality of MediaWiki
Strike MF Piadas admin.php page Parameter PHP File Include	CVE: 2006-3323 BID: 18679	This strike exploits a PHP include flaw in the MF Piadas web application.
Strike Microsoft Visual FoxPro 6 fpole.ocx FoxDoCmd ActiveX Command Execution	BID: 25977 CWE: 78 CVE: 2007-5322	This strike exploits an input sanitization flaw in Microsoft Visual FoxPro 6 that allows arbitrary commands to be executed by the FoxDoCmd method of the fpole.ocx ActiveX control.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Works wkimgsrc.dll WksPictureInterface Memory Corruption	CWE: 20 CVE: 2008-1898 BID: 28820	This strike exploits a memory corruption vulnerability in the Microsoft Works wkimgsrc.dll Activex component.
Strike MiniBB Forum index.php absolute_path Parameter PHP File Include Variant 1	CVE: 2006-3690 BID: 18998	This strike exploits a PHP include flaw in the MiniBB Forum web application.
Strike MiniBB Forum index.php absolute_path Parameter PHP File Include Variant 2	CVE: 2006-3690 BID: 18998	This strike exploits a PHP include flaw in the MiniBB Forum web application.
Strike Modernbill config.php DIR Parameter PHP File Include	CVE: 2006-4034 BID: 19335	This strike exploits a PHP include flaw in the Modernbill web application.
Strike Mozilla compareTo() Arbitrary Code Execution	BID: 14242 CVE: 2005-2265	This strike exploits a code execution vulnerability in the Mozilla Suite, Mozilla Firefox, and Mozilla Thunderbird applications.
Strike Mozilla File Upload Keystroke Hijack	CWE: 200 CVE: 2006-2900 BID: 18308	This strike exploits a user interface misdirection vulnerability in Mozilla browsers (such as Firefox). Due to lax control of the input text field for the file upload widget, a malicious website may redirect keystrokes intended for one element of a frame to the file upload widget. This technique can be used to cause a victim to unknowingly upload a local file to the remote web site.
Strike Mozilla Window Navigator Object Arbitrary Code Execution	BID: 19181 BID: 19192 CWE: 16 CVE: 2006-3677	This strike exploits a code execution vulnerability in the Mozilla Suite, Mozilla Firefox, and Mozilla Thunderbird applications' "navigator" object.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer Cached Objects Zone JavaScript Bypass (showModalDialog)	CVE: 2002-1254 BID: 6028	This strike exploits a flaw in Internet Explorer that allows a script to cache objects and use them to bypass zone restrictions.
Strike Internet Explorer Cached Objects Zone JavaScript Bypass (external)	CVE: 2002-1254 BID: 6028	This strike exploits a flaw in Internet Explorer that allows a script to cache objects and use them to bypass zone restrictions
Strike Internet Explorer Cached Objects Zone JavaScript Bypass (createRange)	CVE: 2002-1254 BID: 6028	This strike exploits a flaw in Internet Explorer that allows a script to cache objects and use them to bypass zone restrictions
Strike Internet Explorer Cached Objects Zone JavaScript Bypass (elementFromPoint)	CVE: 2002-1254 BID: 6028	This strike exploits a flaw in Internet Explorer that allows a script to cache objects and use them to bypass zone restrictions
Strike Internet Explorer Cached Objects Zone JavaScript Bypass (getElementById)	CVE: 2002-1254 BID: 6028	This strike exploits a flaw in Internet Explorer that allows a script to cache objects and use them to bypass zone restrictions
Strike Internet Explorer Cached Objects Zone JavaScript Bypass (getElementsByTagName)	CVE: 2002-1254 BID: 6028	This strike exploits a flaw in Internet Explorer that allows a script to cache objects and use them to bypass zone restrictions
Strike Internet Explorer Cached Objects Zone JavaScript Bypass (getElementsByName)	CVE: 2002-1254 BID: 6028	This strike exploits a flaw in Internet Explorer that allows a script to cache objects and use them to bypass zone restrictions
Strike Internet Explorer Cached Objects Zone JavaScript Bypass (getElementsByTagName)	CVE: 2002-1254 BID: 6028	This strike exploits a flaw in Internet Explorer that allows a script to cache objects and use them to bypass zone restrictions
Strike Internet Explorer Cached Objects Zone JavaScript Bypass (execCommand)	CVE: 2002-1254 BID: 6028	This strike exploits a flaw in Internet Explorer that allows a script to cache objects and use them to bypass zone restrictions
Strike Internet Explorer Cached Objects Zone JavaScript Bypass (clipboardData)	CVE: 2002-1254 BID: 6028	This strike exploits a flaw in Internet Explorer that allows a script to cache objects and use them to bypass zone restrictions

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer Href URL-Encoded Characters Vulnerability	CVE: 2002-1186 BID: 5610	This vulnerability leads to an information disclosure by exploiting a flaw in the way Internet Explorer handles URI encoding
Strike Microsoft Windows Media Services Logging ISAPI Buffer Overflow (121)	CVE: 2003-0227 BID: 7727	This strike exploits a stack-based buffer overflow in Microsoft Windows Media Services via a 121 byte POST to nsiislog.dll which results in remote code execution.
Strike Microsoft Windows Media Services Logging ISAPI Buffer Overflow (5000)	CVE: 2003-0227 BID: 7727	This strike exploits a stack-based buffer overflow in Microsoft Windows Media Services via a 5000 byte POST to nsiislog.dll which results in remote code execution.
Strike Microsoft Windows Media Services Logging ISAPI Buffer Overflow (510)	CVE: 2003-0227 BID: 7727	This strike exploits a stack-based buffer overflow in Microsoft Windows Media Services via a 510 byte POST to nsiislog.dll which results in remote code execution.
Strike Internet Explorer Mishandled OBJECT Tag Type Attribute	CVE: 2003-0344 BID: 7806	This strike exploits a flaw in Internet Explorer's handing of 'type' attributes in 'object' tags
Strike Microsoft IIS nsiilog.dll ISAPI Overflow (25000)	CVE: 2003-0349 BID: 8035	This strike exploits a flaw in nsiislog.dll, an IIS ISAPI filter, by sending a 25000 byte POST request.
Strike Microsoft IIS nsiilog.dll ISAPI Overflow (4354)	CVE: 2003-0349 BID: 8035	This strike exploits a flaw in nsiislog.dll, an IIS ISAPI filter, by sending a 4354 byte POST request.
Strike Microsoft IIS nsiilog.dll ISAPI Overflow (5000)	CVE: 2003-0349 BID: 8035	This strike exploits a flaw in nsiislog.dll, an IIS ISAPI filter, by sending a 5000 byte POST request.
Strike Microsoft Internet Explorer ActiveX Popup Arbitrary Command Execution	CVE: 2003-0838 BID: 8556	This strike exploits a flaw in Microsoft Internet Explorer when displaying web pages that contain malicious popup windows.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer JavaScript XML Object Type Validation Vulnerability	CVE: 2003-0809 BID: 8565	This strike exploits a flaw in internet explorer that loads a malicious URI in the context of the local zone
Strike Microsoft Windows 2000 Troubleshooter JavaScript ActiveX Control Buffer Overflow	CWE: 119 CVE: 2003-0662 BID: 8833	This strike exploits a buffer overflow flaw in the Troubleshooter ActiveX control that is included with Microsoft Windows 2000
Strike IIS Frontpage Extensions Debug Overflow	CVE: 2003-0822 BID: 9007	This strike exploits a buffer overflow in the Frontpage extensions included with IIS.
Strike Help and Support Center Remote Code Execution	CVE: 2004-0199 BID: 10321	This strike generates an HTML page containing a malicious IFRAAME. A browser which processes this IFRAAME will make a Help and Support Center (HCP) request to the local system's HCP DVDUpgrade utility which will then download the requested executable and run it.
Strike Microsoft Windows Compressed Folder Exploit Download (HTTP)	CVE: 2004-0575	This strike exploits a vulnerability in Microsoft Windows when opening a zip file containing a file with a long filename. This strike simulates downloading a malicious zip file via HTTP.
Strike Microsoft Internet Explorer Drag and Drop System File Creation	CVE: 2004-0839 BID: 10973	This strike exploits a vulnerability in Microsoft Internet Explorer that allows a malicious page to write an arbitrary file to the victim host.
Strike Microsoft Internet Explorer Install Engine SetCifFile Heap Overflow	CVE: 2004-0216 BID: 11366	This strike exploits a heap buffer overflow in the Microsoft Internet Explorer Install Engine ActiveX control.
Strike Internet Explorer JavaScript DHTML Object Memory Corruption	CVE: 2005-0553 BID: 13120	This strike exploits a memory corruption flaw in certain DHTML functions in Microsoft Internet Explorer.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer 6 PNG tRNS Chunk Buffer Overflow	CVE: 2005-1211 BID: 13941	This strike exploits a buffer overflow vulnerability in pngfilt.dll for IE6 on WinXP SP2. The buffer overflow occurs while processing the tRNS chunk. Usually, a tRNS chunk must have the same number of entries as the PLTE chunk. If the tRNS chunk has more entries than the PLTE chunk, a buffer may be overflowed, possibly leading to arbitrary code execution.
Strike Microsoft IE javaprx.dll COM instantiation heap overflow	CWE: 399 CVE: 2005-2087 BID: 14087	This strike exploits a heap overflow in Microsoft IE 6, which is triggered when a web page instantiates the javaprx.dll as a COM object
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 1	BID: 14511 CVE: 2005-1990	This strike exploits a flaw in Microsoft Internet Explorer that allows for arbitrary code execution when IE instantiates a COM component as an ActiveX control.
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 4	BID: 14511 CVE: 2005-1990	This strike exploits a flaw in Microsoft Internet Explorer that allows for arbitrary code execution when IE instantiates a COM component as an ActiveX control.
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 6	BID: 14511 CVE: 2005-1990	This strike exploits a flaw in Microsoft Internet Explorer that allows for arbitrary code execution when IE instantiates a COM component as an ActiveX control.
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 10	BID: 14511 CVE: 2005-1990	This strike exploits a flaw in Microsoft Internet Explorer that allows for arbitrary code execution when IE instantiates a COM component as an ActiveX control.
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 11	BID: 14511 CVE: 2005-1990	This strike exploits a flaw in Microsoft Internet Explorer that allows for arbitrary code execution when IE instantiates a COM component as an ActiveX control.
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 13	BID: 14511 CVE: 2005-1990	This strike exploits a flaw in Microsoft Internet Explorer that allows for arbitrary code execution when IE instantiates a COM component as an ActiveX control.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 14	BID: 14511 CVE: 2005-1990	This strike exploits a flaw in Microsoft Internet Explorer that allows for arbitrary code execution when IE instantiates a COM component as an ActiveX control.
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 18	BID: 14511 CVE: 2005-1990	This strike exploits a flaw in Microsoft Internet Explorer that allows for arbitrary code execution when IE instantiates a COM component as an ActiveX control.
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 19	BID: 14511 CVE: 2005-1990	This strike exploits a flaw in Microsoft Internet Explorer that allows for arbitrary code execution when IE instantiates a COM component as an ActiveX control.
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 23	BID: 14511 CVE: 2005-1990	This strike exploits a flaw in Microsoft Internet Explorer that allows for arbitrary code execution when IE instantiates a COM component as an ActiveX control.
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 25	BID: 14511 CVE: 2005-1990	This strike exploits a flaw in Microsoft Internet Explorer that allows for arbitrary code execution when IE instantiates a COM component as an ActiveX control.
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 28	BID: 14511 CVE: 2005-1990	This strike exploits a flaw in Microsoft Internet Explorer that allows for arbitrary code execution when IE instantiates a COM component as an ActiveX control.
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 34	BID: 14511 CVE: 2005-1990	This strike exploits a flaw in Microsoft Internet Explorer that allows for arbitrary code execution when IE instantiates a COM component as an ActiveX control.
Strike Microsoft IE COM Object Embedded CLSID Arbitrary Code Execution Variant 38	BID: 14511 CVE: 2005-1990	This strike exploits a flaw in Microsoft Internet Explorer that allows for arbitrary code execution when IE instantiates a COM component as an ActiveX control.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Windows Media Player Plugin Filename Buffer Overflow	CWE: 119  CVE: 2006-0005  BID: 16644	This strike exploits a buffer overflow vulnerability in the Windows Media Player web browser plugin.
Strike Microsoft Internet Explorer Multiple Event Handler Buffer Overflow	CVE: 2006-1245  BID: 17131	This strike exploits a buffer overflow vulnerability in Microsoft Internet Explorer when rendering an HTML element with many event handlers.
Strike Microsoft Internet Explorer HTML Tag Parsing Memory Corruption Variant 1	CVE: 2006-1188  BID: 17468	This strike exploits a vulnerability in Microsoft Internet Explorer when parsing HTML tags.
Strike Microsoft Internet Explorer HTML Tag Parsing Memory Corruption Variant 2	CVE: 2006-1188  BID: 17468	This strike exploits a vulnerability in Microsoft Internet Explorer when parsing HTML tags.
Strike Microsoft Internet Explorer HTML Tag Parsing Memory Corruption Variant 3	CVE: 2006-1188  BID: 17468	This strike exploits a vulnerability in Microsoft Internet Explorer when parsing HTML tags.
Strike Internet Explorer MDAC RDS.DataSpace ActiveX Code Execution Variant 1	CVE: 2006-0003  BID: 17462	This strike exploits a code execution vulnerability in the RDS DataSpace ActiveX control, using Internet Explorer.
Strike Internet Explorer MDAC RDS.DataSpace ActiveX Code Execution Variant 2	CVE: 2006-0003  BID: 17462	This strike exploits a code execution vulnerability in the RDS DataSpace ActiveX control, using Internet Explorer.
Strike Internet Explorer MDAC RDS.DataSpace ActiveX Code Execution Variant 3	CVE: 2006-0003  BID: 17462	This strike exploits a code execution vulnerability in the RDS DataSpace ActiveX control, using Internet Explorer.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer WMSpecialEffectDX T1Input.bstrPropertyName Memory Corruption	CWE: 94 CVE: 2006-1303 BID: 18328	This strike exploits a vulnerability in Microsoft Internet Explorer when instantiating the wmm2fxa.dll component.
Strike Microsoft Internet Explorer WMSpecialEffectDX TInplace1Input.bstrPropertyName Memory Corruption	CWE: 94 CVE: 2006-1303 BID: 18328	This strike exploits a vulnerability in Microsoft Internet Explorer when instantiating the wmm2fxa.dll component.
Strike Microsoft Internet Explorer WMSpecialEffectDX T2Inputs.bstrPropertyName Memory Corruption	CWE: 94 CVE: 2006-1303 BID: 18328	This strike exploits a vulnerability in Microsoft Internet Explorer when instantiating the wmm2fxa.dll component.
Strike Microsoft Internet Explorer HTML Frameset Memory Corruption	CVE: 2006-3637 BID: 18227	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer when rendering HTML using a crafted frameset.
Strike Microsoft Internet Explorer outerHTML attribute Information Disclosure	CVE: 2006-3280 BID: 18682	This strike exploits an information disclosure vulnerability in Microsoft Internet Explorer when processing javascript that references an object's outerHTML attribute.
Strike Microsoft Internet Explorer HTML Help HHCtrl ActiveX Memory Corruption	CVE: 2006-3357 BID: 18769	This strike exploits a denial of service vulnerability in the HTML Help ActiveX control when setting the image property.
Strike Internet Explorer WebViewFolderIcon ActiveX Control Memory Corruption	CWE: 94 CVE: 2006-3730 BID: 19030	This strike exploits a flaw in the setSlice function of the WebViewFolderIcon ActiveX Object included with Internet Explorer

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Windows Object Packager Dialogue Spoofing (HTTP)	CWE: 94 CVE: 2006-4692 BID: 20318	This strike exploits a dialogue spoofing flaw in the Windows Object Packager. This flaw allows an attacker to embed a malicious object within a RTF or Microsoft Office document that appears to be a safe file type.
Strike Microsoft Internet Explorer DirectAnimation PathControl ActiveX Spline() Method Overflow	CVE: 2006-4446 BID: 19738	This strike exploits a vulnerability in Microsoft Internet Explorer when calling the Spline() method on the DirectAnimation.PathControl ActiveX control.
Strike Microsoft Internet Explorer Daxctle.OCX DirectX KeyFrame Method Overflow	CWE: 119 CVE: 2006-4777 BID: 20047	This strike exploits an overflow in the KeyFrame method of the direct animation DirectX control.
Strike Internet Explorer Daxctle.ocx ActiveX Object KeyFrame Heap Overflow	CWE: 119 CVE: 2006-4777 BID: 20047	This strike exploits a flaw in the DirectX Animation (daxctle.ocx) ActiveX control for Internet Explorer.
Strike Microsoft Internet Explorer XML Object Core Services Memory Corruption	CVE: 2006-5745 BID: 20915	This strike exploits a remote code execution vulnerability in a Microsoft Internet Explorer XML Core Services. Remote attacker can use this vulnerability to do code execution on the target system.
Strike Internet Explorer WMI Object Broker ActiveX Code Execution Variant 1	BID: 20843 CVE: 2006-4704	This strike exploits a code execution vulnerability in the WMI Object Broker ActiveX control, using Internet Explorer.
Strike Internet Explorer WMI Object Broker ActiveX Code Execution Variant 2	BID: 20843 CVE: 2006-4704	This strike exploits a code execution vulnerability in the WMI Object Broker ActiveX control, using Internet Explorer.
Strike Internet Explorer WMI Object Broker ActiveX Code Execution Variant 3	BID: 20843 CVE: 2006-4704	This strike exploits a code execution vulnerability in the WMI Object Broker ActiveX control, using Internet Explorer.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Windows Media Player ASX File Heap Overflow (HTTP)	CWE: 119 CVE: 2006-6134 BID: 21247	Microsoft Windows Media Player contains a vulnerability that will cause memory corruption when a malicious *.asx file is opened
Strike Internet Explorer VML Object Buffer Overflow	CVE: 2007-0024 BID: 21930	This strike exploits a buffer overflow flaw in the VML features of Internet Explorer
Strike Microsoft Word 2000 Malformed Function Code Execution (HTTP)	CVE: 2007-0515 BID: 22225	This strike exploits a code execution flaw in Microsoft Word 2000 that is triggered by a malformed function definition.
Strike Windows Animated Cursor (.ani) Handling Arbitrary Command Execution (HTTP)	CWE: 119 CVE: 2007-0038 BID: 23194	This strike exploits a code execution vulnerability in the Microsoft Windows animated cursor (.ani) file handling function.
Strike Microsoft Internet Explorer chtskdic.dll COM Object Instantiation Memory Corruption	CVE: 2007-0942 BID: 19529	Microsoft Internet Explorer 5.01 SP4 on Windows 2000 SP4; 6 SP1 on Windows 2000 SP4; 6 and 7 on Windows XP SP2, or Windows Server 2003 SP1 or SP2; and possibly 7 on Windows Vista does not properly instantiate certain COM objects as ActiveX controls, which allows remote attackers to execute arbitrary code via a crafted COM object from chtskdic.dll.
Strike BizTalk CAPICOM Certificates ActiveX Control Remote Code Execution	CVE: 2007-0940 BID: 23782	This strike exploits a memory corruption vulnerability in the CAPICOM ActiveX control included with BizTalk 2004.
Strike Microsoft Visio File Version Code Execution (HTTP)		This strike exploits an arbitrary code execution flaw in Microsoft Visio 2002. The vulnerability is triggered when a version is specified that is less than six and greater than zero.
Strike Internet Explorer COM Object Instantiation Pointer Memory Corruption Variant 1	BID: 24372 CWE: 94 CVE: 2007-0218	This strike exploits a memory corruption issue in Internet Explorer triggered by an uninitialized pointer returned via a malicious COM object instantiation.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer COM Object Instantiation Pointer Memory Corruption Variant 2	BID: 24372 CWE: 94 CVE: 2007-0218	This strike exploits a memory corruption issue in Internet Explorer triggered by an uninitialized pointer returned via a malicious COM object instantiation.
Strike Internet Explorer COM Object Instantiation Pointer Memory Corruption Variant 3	BID: 24372 CWE: 94 CVE: 2007-0218	This strike exploits a memory corruption issue in Internet Explorer triggered by an uninitialized pointer returned via a malicious COM object instantiation.
Strike Internet Explorer COM Object Instantiation Pointer Memory Corruption Variant 4	BID: 24372 CWE: 94 CVE: 2007-0218	This strike exploits a memory corruption issue in Internet Explorer triggered by an uninitialized pointer returned via a malicious COM object instantiation.
Strike Internet Explorer COM Object Instantiation Pointer Memory Corruption Variant 5	BID: 24372 CWE: 94 CVE: 2007-0218	This strike exploits a memory corruption issue in Internet Explorer triggered by an uninitialized pointer returned via a malicious COM object instantiation.
Strike Internet Explorer COM Object Instantiation Pointer Memory Corruption Variant 6	BID: 24372 CWE: 94 CVE: 2007-0218	This strike exploits a memory corruption issue in Internet Explorer triggered by an uninitialized pointer returned via a malicious COM object instantiation.
Strike Internet Explorer CSS Style Tag Memory Corruption	CVE: 2007-1750 CVE: 2007-0943	This strike exploits a flaw in Internet Explorer 6 caused by an invalid 'csstext' property in the 'style' attribute of an HTML tag.
Strike Internet Explorer Navigation Cancel Page XSS (About)	BID: 22966 CWE: 79 CVE: 2007-1499	This strike exploits a cross-site scripting flaw in Internet Explorer 7. This flaw can be used by an attacker to spoof the displayed document location and run javascript code in the context of the about:cancel context.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer Navigation Cancel Page XSS (Res)	BID: 22966 CWE: 79 CVE: 2007-1499	This strike exploits a cross-site scripting flaw in Internet Explorer 7. This flaw can be used by an attacker to spoof the displayed document location and run javascript code in the context of the about:cancel context.
Strike Internet Explorer Microsoft Speech API 4 ActiveX Overflow	BID: 24426 CWE: 119 CVE: 2007-2222	This strike exploits an overflow in the Microsoft Speech API version 4 using an ActiveX control
Strike Internet Explorer Windows API Resource ID Arbitrary Code Execution	BID: 24370 CVE: 2007-2219	This strike exploits a flaw in the Microsoft Windows API using Internet Explorer. This flaw is triggered when a resource URL is specified that contains an ID greater than 65535. A logic error results in the resource ID being treated as a pointer to a resource and deallocated using the RtlFreeHeap() function. Since the attacker controls the value of this ID, this can lead to code execution.
Strike Microsoft IIS ASP.NET NULL Byte Injection Information Disclosure Variant 1	BID: 24791 CWE: 200 CVE: 2007-0042	This strike bypasses the security features of an ASP.NET website by injecting a NULL character into the request URI.
Strike Microsoft IIS ASP.NET NULL Byte Injection Information Disclosure Variant 2	BID: 24791 CWE: 200 CVE: 2007-0042	This strike bypasses the security features of an ASP.NET website by injecting a NULL character into the request URI.
Strike Microsoft IIS ASP.NET NULL Byte Injection Information Disclosure Variant 3	BID: 24791 CWE: 200 CVE: 2007-0042	This strike bypasses the security features of an ASP.NET website by injecting a NULL character into the request URI.
Strike Microsoft IIS ASP.NET NULL Byte Injection Information Disclosure Variant 4	BID: 24791 CWE: 200 CVE: 2007-0042	This strike bypasses the security features of an ASP.NET website by injecting a NULL character into the request URI.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft XML Core Services substringData Attribute Integer Overflow	BID: 25301 CWE: 119 CVE: 2007-2223	This strike exploits an integer overflow vulnerability in the Microsoft XML Core Services control. This flaw is a combination of improper input validation in the XML software (MS07-042) and an integer overflow in the OLE Automation Library (MS07-043).
Strike Microsoft Internet Explorer Pdwizard.ocx ActiveX Object Memory Corruption	CVE: 2007-3041 BID: 25295	Unspecified vulnerability in the pdwizard.ocx ActiveX object for Internet Explorer 5.01, 6 SP1, and 7 allows remote attackers to execute arbitrary code via unknown vectors related to Microsoft Visual Basic 6 objects and memory corruption, aka "ActiveX Object Memory Corruption Vulnerability."
Strike Internet Explorer TLBINFO32.DLL Remote DLL Loading Code Execution Vulnerability	BID: 25289 CWE: 16 CVE: 2007-2216	This strike uses tlbinfo32.dll to load a malicious DLL from the remote machine and use it to execute code on the target machine.
Strike Windows GDI Malformed Image Denial of Service (HTTP)	BID: 25302 CWE: 189 CVE: 2007-3034	This strike exploits a denial-of-service vulnerability in Windows when handling malformed WMF files
Strike Microsoft Windows Vista Contact Gadget Remote Code Execution (HTTP)	CVE: 2007-3032 BID: 25304	This strike exploits a flaw in the Contact Gadget in Microsoft Vista when displaying a malicious contact.
Strike Microsoft Windows Vista RSS Feed Headlines Gadget Remote Code Execution Variant 1	CWE: 79 CVE: 2007-3033 BID: 25287	This strike exploits a flaw in the Feed Headlines Gadget in Microsoft Vista when displaying a malicious RSS feed.
Strike Microsoft Windows Vista RSS Feed Headlines Gadget Remote Code Execution Variant 2	CWE: 79 CVE: 2007-3033 BID: 25287	This strike exploits a flaw in the Feed Headlines Gadget in Microsoft Vista when displaying a malicious RSS feed.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Kodak Image Viewer TIFF BE File Parsing Code Execution (HTTP)	BID: 25909 CWE: 94 CVE: 2007-2217	This strike exploits a code execution vulnerability in the Kodak Image Viewer's TIFF (.tif) file handling function.
Strike Kodak Image Viewer TIFF LE File Parsing Code Execution (HTTP)	BID: 25909 CWE: 94 CVE: 2007-2217	This strike exploits a code execution vulnerability in the Kodak Image Viewer's TIFF (.tif) file handling function.
Strike Microsoft Windows PDF URI Handling Arbitrary Command Execution (HTTP)	CWE: 94 CVE: 2007-5020 BID: 25748	This strike exploits a command execution vulnerability in Microsoft Windows XP and 2003 URI handling via the Adobe Acrobat 8.x PDF (.pdf) "mailto" URI object's resolving functionality when paired with IE7 as the default URI handler.
Strike Microsoft DirectShow SAMI XML Attribute Overflow	CWE: 119 CVE: 2007-3901 BID: 26789	This strike exploits a bug in quartz.dll of DirectShow that gets triggered by a SAMI (closed captioning) file with an XML attribute that is very long
Strike Microsoft IIS ASP Engine HTMLEncode() Buffer Overflow	BID: 27676 CWE: 94 CVE: 2008-0075	This strike exploits a buffer overflow in the HTMLEncode function provided with the ASP scripting engine. This particular strike exploits this flaw through a sample script provided with the popular FCKeditor component.
Strike Microsoft Visual FoxPro ActiveX FoxDoCmd Control Buffer Overflow	CWE: 119 CVE: 2007-4790 BID: 25571	This strike exploits a buffer overflow in a Microsoft Visual FoxPro Activex control when calling the FoxDoCmd function.
Strike Microsoft Internet Explorer SVG AnimateMotion Memory Corruption	BID: 27666 CWE: 399 CVE: 2008-0077	This strike exploits a memory corruption bug in Microsoft Internet Explorer when rendering malicious SVG content.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Works RTF File Conversion Buffer Overflow (HTTP)	BID: 27659 CWE: 119 CVE: 2008-0108	This strike exploits a buffer overflow in the Microsoft Office and Microsoft Works file converter. A buffer overflow can be triggered when a corrupted Microsoft Works file is converted to the Rich Text Format (RTF).
Strike Microsoft Outlook mailto URI Argument Injection (altvba)	CWE: 94 CVE: 2008-0110 BID: 28147	This strike exploits a argument injection vulnerability in Microsoft Outlook. This flaw can be used to execute arbitrary code via the /altvba and /importprf options.
Strike Microsoft Outlook mailto URI Argument Injection (importprf)	CWE: 94 CVE: 2008-0110 BID: 28147	This strike exploits a argument injection vulnerability in Microsoft Outlook. This flaw can be used to execute arbitrary code via the /altvba and /importprf options.
Strike Microsoft Office Memory Corruption (PowerPoint) (HTTP)	BID: 28146 CWE: 94 CVE: 2008-0118	This strike exploits a memory corruption vulnerability in the Microsoft Office XP PowerPoint component.
Strike Microsoft Windows GDI Stack Overflow (HTTP)	BID: 28570 CWE: 119 CVE: 2008-1087	This strike sends a file that exploits a stack overflow flaw in GDI, a core component of the Microsoft Windows Graphical User Interface
Strike Internet Explorer Same-Origin XMLHttpRequest Header Forgery	CWE: 20 CVE: 2008-1544 BID: 28379	This strike exploits a vulnerability in the blocklisting mechanism employed by Internet Explorer 7 to enforce the same-origin policy for embedded XMLHttpRequest objects. Due to a problem in data sanitation, an attacker can use maliciously-crafted setRequestHeader() calls to an XMLHttpRequest objects to overwrite certain HTTP request headers.
Strike Internet Explorer Malicious SpSharedRecoContext ActiveX Illegal Instantiation	CWE: 94 CVE: 2007-0675 BID: 22359	This strike exploits a malicious instantiation of the Microsoft Speech Recognition 'SpSharedRecoContext' ActiveX control. The kill bit for this control has been issued by Microsoft in bulletin MS08-32, as this control is not intended to be invoked by Internet Explorer.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer Malicious SpSharedRecognizer ActiveX Illegal Instantiation	CWE: 94 CVE: 2007-0675 BID: 22359	This strike exploits a malicious instantiation of the Microsoft Speech Recognition 'SpSharedRecognizer' ActiveX control. The kill bit for this control has been issued by Microsoft in bulletin MS08-32, as this control is not intended to be invoked by Internet Explorer.
Strike DirectX AVI-ASF MJPEG Decoding Code Execution (HTTP)	BID: 29581 CWE: 119 CVE: 2008-0011	This strike exploits a code execution vulnerability in the DirectX MJPEG decoding component.
Strike Microsoft DirectShow SAMI CSS Attribute Overflow	CWE: 119 CVE: 2008-1444 BID: 29578	This strike exploits a bug in quartz.dll of DirectShow that gets triggered by a SAMI (closed captioning) file with an CSS attribute that is very long. CyPerf was unable to reproduce this vulnerability in its lab.
Strike Internet Explorer - Snapshot Viewer for Microsoft Access ActiveX Arbitrary File Download Variant 2	CWE: 94 CVE: 2008-2463 BID: 30114	This strike exploits a malicious instantiation of the Snapshot Viewer for Microsoft Access ActiveX control. Due to a design error, a malicious web page may silently download executable files from an Internet site to any location on the victim's hard drive, including auto-start extensibility points (ASEPs). These programs, in turn, may then silently run with the privileges of the currently-logged on user.
Strike Internet Explorer - Snapshot Viewer for Microsoft Access ActiveX Arbitrary File Download Variant 3	CWE: 94 CVE: 2008-2463 BID: 30114	This strike exploits a malicious instantiation of the Snapshot Viewer for Microsoft Access ActiveX control. Due to a design error, a malicious web page may silently download executable files from an Internet site to any location on the victim's hard drive, including auto-start extensibility points (ASEPs). These programs, in turn, may then silently run with the privileges of the currently-logged on user.
Strike Internet Explorer - Snapshot Viewer for Microsoft Access ActiveX Arbitrary File Download Variant 4	CWE: 94 CVE: 2008-2463 BID: 30114	This strike exploits a malicious instantiation of the Snapshot Viewer for Microsoft Access ActiveX control. Due to a design error, a malicious web page may silently download executable files from an Internet site to any location on the victim's hard drive, including auto-start extensibility points (ASEPs). These programs, in turn, may then silently run with the privileges of the currently-logged on user.
Strike Microsoft Office Smart Tag WordCount Memory Corruption (HTTP)	BID: 30124 CWE: 399 CVE: 2008-2244	This strike exploits a memory corruption vulnerability in Microsoft Office that is triggered when a Smart Tag structure containing an invalid WordCount value.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Excel Chart Record Array Index Vulnerability (HTTP)	BID: 30638 CWE: 20 CVE: 2008-3004	This strike exploits a code execution vulnerability in Microsoft Excel caused by loading a workbook with a malicious record.
Strike Microsoft Office Graphics Image Filter PICT Heap Overflow	BID: 30597 CWE: 94 CVE: 2008-3018	This strike exploits a heap-based buffer overflow in the Microsoft Office Graphics Image Filter for the PICT file format.
Strike Microsoft Office Graphics Image Filter PICT NULL Pointer Dereference	BID: 30598 CWE: 399 CVE: 2008-3021	This strike exploits a NULL pointer dereference in the Microsoft Office Graphics Image Filter for the PICT file format.
Strike Microsoft Office Graphics Image Filter PICT Memory Corruption (Fatal)	BID: 30598 CWE: 399 CVE: 2008-3021	This strike exploits a NULL pointer dereference in the Microsoft Office Graphics Image Filter for the PICT file format. This differs from the normal trigger for this exploit in that it is not wrapped by an exception filter and results in a fatal crash of the Office application.
Strike Microsoft Office Graphics Image Filter WPG Heap Overflow	BID: 30600 CWE: 399 CVE: 2008-3460	This strike exploits a heap overflow in the Microsoft Office Graphics Image Filter for the WPG file format.
Strike Internet Explorer HTML createTextRange() Memory Corruption	CWE: 399 CVE: 2008-2255	This strike exploits a memory corruption issue in Internet Explorer triggered by rapid calls to createTextRange().
Strike Internet Explorer ExecWB PrintPreview Remote Command Execution	BID: 30612 CWE: 20 CVE: 2008-2259	This strike exploits an insecure API call in Internet Explorer that enables scripting to run in the local zone.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer HTML Objects Uninitialized Memory	BID: 30614 CWE: 399 CVE: 2008-2254	This strike causes Internet Explorer to access uninitialized memory.
Strike Internet Explorer HTML Table Objects Memory Corruption	BID: 30610 CWE: 399 CVE: 2008-2258	This strike uses HTML Table objects to cause a memory corruption issue with Internet Explorer.
Strike Internet Explorer HTTP Code 449 Uninitialized Object Memory Corruption Vulnerability	BID: 30611 CWE: 20 CVE: 2008-2256	This strike replies to an HTTP request with code 449 (Retry) which will cause certain versions of Internet Explorer to crash.
Strike Internet Explorer Nested XHTML Object Memory Corruption	BID: 30613 CWE: 399 CVE: 2008-2257	This strike exploits a flaw in Internet Explorer caused by uninitialized memory and nested XHTML objects.
Strike Microsoft Color Management ColorMatchToTarget W (HTTP)	BID: 30594 CWE: 119 CVE: 2008-2245	This strike exploits a memory corruption vulnerability in the Microsoft Windows Color Management System when handling EMF files with a crafted EMR_COLORMATCHTOTARGETW record.
Strike Internet Explorer MHTML HTTP Redirect Cross Domain Information Disclosure	BID: 30585 CWE: 264 CVE: 2008-1448	This strike uses an MHTML redirect to cause Internet Explorer to allow script access to domains other than the originating site.
Strike Internet Explorer MSN Messenger ActiveX Control Information Disclosure Variant 1	BID: 30551 CWE: 200 CVE: 2008-0082	This strike exploits an information disclosure vulnerability present in Microsoft's MSN Messenger "Messenger.UIAutomation" ActiveX control. Due to a lack of controls around certain API functions, a malicious web page can harvest personally- identifying information without consent or notification to the user, including e-mail addresses and MSN screen names.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer MSN Messenger ActiveX Control Information Disclosure Variant 2	BID: 30551 CWE: 200 CVE: 2008-0082	This strike exploits an information disclosure vulnerability present in Microsoft's MSN Messenger "Messenger.UIAutomation" ActiveX control. Due to a lack of controls around certain API functions, a malicious web page can harvest personally- identifying information without consent or notification to the user, including e-mail addresses and MSN screen names.
Strike Microsoft PowerPoint Master Style Integer Overflow (HTTP)	BID: 30579 CWE: 399 CVE: 2008-1455	This strike exploits a memory corruption vulnerability in Microsoft PowerPoint when opening a file with a malformed Master Style attribute.
Strike Microsoft PowerPoint Viewer 2003 Picture Array Index (HTTP)	BID: 30552 CWE: 399 CVE: 2008-0120	This strike exploits an out-of-bounds array index vulnerability in Microsoft PowerPoint Viewer 2003 when reading malformed PowerPoint files.
Strike Microsoft PowerPoint Viewer 2003 MSODRAWING Property Heap Overflow (HTTP)	BID: 30554 CWE: 399 CVE: 2008-0121	This strike exploits a memory corruption vulnerability in Microsoft PowerPoint Viewer when processing a file with a malformed MSODRAWING Property Table.
Strike Microsoft GDI+ BMP Integer Overflow (HTTP)	BID: 31022 CWE: 189 CVE: 2008-3015	This strike exploits a BMP parsing flow caused by an invalid image width.
Strike Microsoft Internet Explorer Malformed GDI+ EMF Memory Corruption	BID: 31019 CWE: 119 CVE: 2008-3012	This strike exploits a memory corruption bug in Microsoft Internet Explorer when viewing EMF files containing a malformed floating point field.
Strike Microsoft Internet Explorer GDI+ GIF Parsing Record Count Memory Corruption	BID: 31020 CWE: 399 CVE: 2008-3013	This strike exploits a memory corruption bug in Microsoft Internet Explorer when parsing GIF files with a large number of GIF records.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer GDI+ VML Gradient Negative Focussize Variant 1	BID: 31018 CWE: 189 CVE: 2007-5348	This strike exploits an integer overflow bug in Microsoft Internet Explorer when rendering VML that contains negative FocusSize values.
Strike Microsoft Internet Explorer GDI+ VML Gradient Negative Focussize Variant 2	BID: 31018 CWE: 189 CVE: 2007-5348	This strike exploits an integer overflow bug in Microsoft Internet Explorer when rendering VML that contains negative FocusSize values.
Strike Microsoft Windows Media Encoder IE ActiveX Control Overflow	BID: 31065 CWE: 119 CVE: 2008-3008	This strike exploits an overflow in the Windows Media Encoder ActiveX Control using Internet Explorer as a vector.
Strike Microsoft OneNote URI Handler Injection Arbitrary File Write	BID: 31067 CWE: 20 CVE: 2008-3007	This strike will load a malicious HTML file that will connect to a remote server, download an Office OneNote file, and save any inserted files to a directory specified by the malicious author.
Strike Microsoft Excel BIFF Record Parsing Vulnerability (HTTP)	BID: 31705 CWE: 399 CVE: 2008-3471	This strike exploits a vulnerability in Microsoft Excel when parsing a file containing crafted BIFF records.
Strike Microsoft Excel Embedded Object Validation Vulnerability (HTTP)	BID: 31702 CWE: 399 CVE: 2008-3477	This strike exploits a vulnerability in Microsoft Excel when parsing a file containing an embedded object.
Strike Microsoft Excel REPT() Formula Parsing Vulnerability (HTTP)	BID: 31706 CWE: 189 CVE: 2008-4019	This strike exploits a vulnerability in Microsoft Excel when evaluating a REPT() formula with a long number_times parameter.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer Cross Domain Cookie Theft Variant 1	BID: 31615 BID: 31654 CWE: 264 CVE: 2008-3472	This strike exploits an information disclosure vulnerability present in Microsoft Internet Explorer. Due to an issue in enforcing the same-origin policy within Internet Explorer, a malicious web page can read from and write to the content of a child iframe. Using this vulnerability, an attacker can interact with the child frame on behalf of the user without further user interaction.
Strike Microsoft Internet Explorer Cross Domain Cookie Theft Variant 2	BID: 31616 CWE: 264 CVE: 2008-3473	This strike exploits an information disclosure vulnerability present in Microsoft Internet Explorer. Due to an issue in enforcing the same-origin policy within Internet Explorer, a malicious web page can read from and write to the content of a child iframe. Using this vulnerability, an attacker can interact with the child frame on behalf of the user without further user interaction.
Strike Microsoft Internet Explorer Cross Domain Cookie Theft Variant 3	CWE: 284 CVE: 2008-2947 BID: 29986	This strike exploits an information disclosure vulnerability present in Microsoft Internet Explorer. Due to an issue in enforcing the same-origin policy within Internet Explorer, a malicious web page can change the location of a pop-up window or frame. Using this vulnerability, an attacker can interact with the window or frame on behalf of the user without further user interaction.
Strike Internet Explorer DOM XML Heap Corruption Variant 1	BID: 31617 CWE: 399 CVE: 2008-3475	This strike exploits a heap memory corruption vulnerability present in Microsoft Internet Explorer. Due to a misallocation of memory during certain DOM manipulation actions, a malicious web page can cause an exception within Internet Explorer.
Strike Internet Explorer DOM XML Heap Corruption Variant 2	BID: 31618 CWE: 399 CVE: 2008-3476	This strike exploits a heap memory corruption vulnerability present in Microsoft Internet Explorer. Due to a misallocation of memory during certain DOM manipulation actions, a malicious web page can cause an exception within Internet Explorer.
Strike Microsoft XML Core Services DTD Cross-Domain Scripting External Parameter Entity	BID: 32155 CWE: 200 CVE: 2008-4029	This strike simulates a cross-domain scripting vulnerability in Microsoft XML Core Services that occurs when Microsoft Internet Explorer uses the MSXML ActiveX control to load a DTD with an external parameter entity.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Visual Basic Charts ActiveX Control DoSetCursor Parameter Memory Corruption	BID: 32614 CWE: 399 CVE: 2008-4256	This strike simulates an attack against the Visual Basic 6.0 Charts ActiveX Control that is triggered when setting the DoSetCursor parameter.
Strike Microsoft Visual Basic DataGrid ActiveX Control Text Parameter Memory Corruption	BID: 32591 CWE: 264 CVE: 2008-4252	This strike simulates an attack against the Visual Basic 6.0 DataGrid ActiveX Control that is triggered when setting the Text parameter.
Strike Microsoft Visual Basic FlexGrid ActiveX Control FormatString Parameter Memory Corruption	BID: 32592 CWE: 399 CVE: 2008-4253	This strike simulates an attack against the Visual Basic 6.0 FlexGrid ActiveX Control that is triggered when setting the FormatString parameter.
Strike Microsoft Visual Basic Hierarchical FlexGrid ActiveX Control Rows Parameter Memory Corruption	CWE: 189 CVE: 2008-4254	This strike simulates an attack against the Visual Basic 6.0 Hierarchical FlexGrid ActiveX Control that is triggered when setting the Rows parameter.
Strike Microsoft Visual Basic Masked Edit ActiveX Control Mask Parameter Memory Corruption	CWE: 119 CVE: 2008-3704 BID: 30674	This strike simulates an attack against the Visual Basic 6.0 Masked Edit ActiveX Control that is triggered when setting the Mask parameter.
Strike Microsoft GDI DIBBITBLT HeaderSize Integer Overflow (HTTP)	CWE: 189 CVE: 2008-2249	This strike exploits an integer overflow when handling the HeaderSize value from the DIBHeader structure contained within a Widows Meta File (WMF) DIBBITBLT record.
Strike Microsoft GDI DIBSTRETCHBLT HeaderSize Integer Overflow (HTTP)	CWE: 189 CVE: 2008-2249	This strike exploits an integer overflow when handling the HeaderSize value from the DIBHeader structure contained within a Widows Meta File (WMF) DIBSTRETCHBLT record.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Word RTF Object Parsing Vulnerability (HTTP)	CWE: 399 CVE: 2008-4027	This strike exploits a vulnerability in MS Word caused by an RTF file with invalid '\do' directives.
Strike Microsoft Word RTF Object Parsing Vulnerability (dpcallout) (HTTP)	CWE: 119 CVE: 2008-4028	This strike exploits a vulnerability in MS Word caused by an RTF file with invalid '\dpcallout' directives.
Strike Microsoft Word RTF Object Parsing Vulnerability (dpPENDGROUP) (HTTP)	CWE: 399 CVE: 2008-4030	This strike exploits a vulnerability in MS Word caused by an RTF file with invalid '\dpPENDGROUP' directives.
Strike Microsoft Word RTF Object Parsing Vulnerability (dpolycount) (HTTP)	CWE: 119 CVE: 2008-4025	This strike exploits a vulnerability in MS Word caused by an RTF file with an invalid '\dpolycount' directive.
Strike Microsoft Word RTF Object Parsing Vulnerability (stylesheet) (HTTP)	CWE: 399 CVE: 2008-4031	This strike exploits a vulnerability in MS Word caused by an RTF file with invalid '\stylesheet' directives.
Strike Microsoft Word Memory Corruption Vulnerability (HTTP) (Array Index)	CWE: 399 CVE: 2008-4026	This strike exploits a vulnerability in MS Word that uses an unchecked offset into an array.
Strike Microsoft Word Memory Corruption Vulnerability (HTTP) (Arbitrary Free)	CWE: 94 CVE: 2008-4024	This strike exploits a vulnerability in MS Word that allows a malicious document to run 'free()' on an arbitrary address.
Strike Microsoft Word Table Property Stack Overflow (HTTP)	CWE: 119 CVE: 2008-4837	This strike exploits a vulnerability in MS Word caused when processing an invalid table property.
Strike Internet Explorer HTML Iframe Object Buffer Overflow	CWE: 399 CVE: 2008-4259	This strike exploits a buffer overflow vulnerability present in Microsoft Internet Explorer. Due to an issue involving certain HTML objects, a malicious web page can overflow a static buffer, leading to system instability and the possibility of remote code execution.

Name	References	Description
Strike Internet Explorer HTML Embed Rendering Buffer Overflow	CWE: 399 CVE: 2008-4261	This strike exploits a buffer overflow vulnerability present in Microsoft Internet Explorer. Due to an issue rendering certain HTML elements, a malicious web page can supply malicious data via Internet Explorer, leading to system instability and the possibility of remote code execution.
Strike Internet Explorer Navigation Parameter Buffer Overflow Variant 1	CWE: 399 CVE: 2008-4258 BID: 32596	This strike exploits a buffer overflow vulnerability present in Microsoft Internet Explorer. Due to an issue involving web site navigation, a malicious web page can cause Internet Explorer to miscalculate the buffer size required for certain elements, leading to system instability and the possibility of remote code execution.
Strike Internet Explorer Navigation Parameter Buffer Overflow Variant 2	CWE: 399 CVE: 2008-4258 BID: 32596	This strike exploits a buffer overflow vulnerability present in Microsoft Internet Explorer. Due to an issue involving web site navigation, a malicious web page can cause Internet Explorer to miscalculate the buffer size required for certain elements, leading to system instability and the possibility of remote code execution.
Strike Microsoft Excel Obj Record Invalid Subtype Vulnerability (HTTP)	BID: 32621 CWE: 399 CVE: 2008-4264	This strike exploits a vulnerability in Microsoft Excel when parsing a file containing an embedded object with an invalid subtype record.
Strike Microsoft Windows Search search-ms URL Protocol Handler Vulnerability	CWE: 399 CVE: 2008-4269	This strike exploits a vulnerability in Windows Internet Explorer when opening a malicious URL using the search-ms protocol.
Strike Microsoft Internet Explorer XML Data Binding Memory Corruption	CWE: 399 CVE: 2008-4844 BID: 32721	This strike simulates a memory corruption flaw in Microsoft Internet Explorer's data binding functionality. This vulnerability was discovered in the wild.
Strike Internet Explorer Cascading Style Sheet Visibility Manipulation Buffer Overflow	BID: 33627 CWE: 399 CVE: 2009-0075	This strike exploits a buffer overflow vulnerability present in Microsoft Internet Explorer. Due to an issue handling certain span and block elements when they are manipulated via CSS after they have been rendered in the DOM, a malicious web page can trigger an uninitialized memory corruption condition in Internet Explorer, leading to system instability and remote code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Internet Explorer DOM Deleted Object Buffer Overflow	BID: 33627 CWE: 399 CVE: 2009-0075	This strike exploits a buffer overflow vulnerability present in Microsoft Internet Explorer. Due to an issue handling certain objects after they are deleted from the Document Object Model (DOM), a malicious web page can trigger an uninitialized memory corruption condition in Internet Explorer, leading to system instability and remote code execution.
Strike Microsoft Windows EMF Polyline (HTTP)	BID: 34012 CWE: 20 CVE: 2009-0081	This strike exploits a vulnerability in Microsoft Windows when parsing an EMF file with crafted EMR_POLYLINE data.
Strike Microsoft Office Text Converter Integer Underflow Code Execution (HTTP Corrupt)	CVE: 2009-0087	This strike exploits an integer underflow code execution vulnerability in Microsoft Office's text convertor.
Strike Microsoft Office Text Converter Integer Underflow Code Execution (HTTP Direct)	CVE: 2009-0087	This strike exploits an integer underflow code execution vulnerability in Microsoft Office's text convertor.
Strike Internet Explorer - Uninitialized Memory Corruption Vulnerability Variant 1	CWE: 94 CVE: 2009-0552	This strike exploits an uninitialized memory corruption vulnerability present in Microsoft Internet Explorer. Due to an issue in accessing a memory location which has not been properly initialized, a malicious web page can trigger a double-free heap corruption condition in Internet Explorer, leading to system instability and remote code execution.
Strike Internet Explorer - Uninitialized Memory Corruption Vulnerability Variant 2	CWE: 399 CVE: 2009-0554	This strike exploits an uninitialized memory corruption vulnerability present in Microsoft Internet Explorer. Due to an issue in accessing a memory location which has not been properly initialized, a malicious web page can trigger an access violation condition in Internet Explorer, leading to system instability and remote code execution.
Strike Internet Explorer - Uninitialized Memory Corruption Vulnerability Variant 3	BID: 34424 CWE: 399 CVE: 2009-0553	This strike exploits an uninitialized memory corruption vulnerability present in Microsoft Internet Explorer. Due to an issue in accessing a memory location which has not been properly initialized, a malicious web page can trigger a double-free heap corruption condition in Internet Explorer, leading to system instability and remote code execution.
Strike ISA Server 2006 XSS in CookieAuth.dll	CWE: 79 CVE: 2009-0237	A cross-site scripting vulnerability exists in Microsoft ISA Server 2006.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft PowerPoint Current User Length Buffer Overflow (HTTP)	BID: 34841 CWE: 119 CVE: 2009-1131	This strike exploits a stack overflow vulnerability in Microsoft PowerPoint that is triggered by a Current user object with a length greater than 255 bytes.
Strike Microsoft Office PowerPoint 7 Converter Code Execution (HTTP)	BID: 34837 CWE: 94 CVE: 2009-1128	This strike exploits a code execution vulnerability in Microsoft Office PowerPoint's PowerPoint 7 converter.
Strike Microsoft Office PowerPoint Code Execution (HTTP)	BID: 34840 CWE: 119 CVE: 2009-1130	This strike exploits a code execution vulnerability in Microsoft Office PowerPoint.
Strike Microsoft PowerPoint TextHeaderAtom Freed Memory Heap Corruption (HTTP)	BID: 34351 CWE: 94 CVE: 2009-0556	This strike exploits a heap memory corruption vulnerability in Microsoft Office's PowerPoint.
Strike Microsoft Office PP7 Stack Overflow Vulnerability (HTTP)	BID: 34839 CWE: 119 CVE: 2009-1129	This strike exploits a stack overflow vulnerability in Microsoft Office PowerPoint when viewing a crafted PowerPoint document.
Strike Internet Explorer DHTML Table Object Memory Corruption	CWE: 399 CVE: 2009-1141 BID: 35198	This strike exploits a flaw in Internet Explorer that causes a memory corruption issue when encountering malicious DHTML.
Strike Microsoft Internet Explorer 8 DOM Object Dangling Pointer Memory Corruption	CWE: 399 CVE: 2009-1532	This strike exploits a flaw in Internet Explorer's handling of certain DOM Objects that can result in code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Office Excel OBJ Record Parsing Remote Code Execution (HTTP)	CWE: 94 CVE: 2009-0557 BID: 34351	This strike sends a malicious Office Excel document that can execute arbitrary code.
Strike Microsoft DirectShow Large ImageDescription Name Size Code Execution (HTTP)	BID: 35139 CVE: 2009-1537	This strike exploits a vulnerability in Microsoft DirectShow when parsing a media file containing maliciously formatted QuickTime data.
Strike Microsoft Embedded OpenType Font Parser Code Execution (HTTP)	CWE: 119 CVE: 2009-0231	This strike exploits a vulnerability in Microsoft's Embedded OpenType file parsing engine when parsing an EOT file containing malicious OpenType font file structure data.
Strike Microsoft ASP.NET Request Scheduling DoS	BID: 35985 CWE: 20 CVE: 2009-1536	This strike exploits a DoS bug in the Microsoft .NET Framework via IIS with ASP.NET configured to use integrated mode.
Strike Microsoft DirectShow (msvidctl.dll) MPEG-2 Memory Corruption	BID: 35558 BID: 35585 CWE: 119 CVE: 2008-0015	This strike exploits a memory corruption vulnerability in the MSVidCtl component of Microsoft DirectShow. An attacker can use a malicious GIF file to trigger a buffer overflow and execute arbitrary code.
Strike Microsoft Windows AVIFile Media File Truncation Code Execution (HTTP)	BID: 35967 CWE: 94 CVE: 2009-1545	This strike exploits a vulnerability in Microsoft Windows when parsing an AVI file with truncated AVIH chunk data.
Strike Microsoft OWC Spreadsheet ActiveX Control Memory Corruption	CWE: 94 CVE: 2009-1136	This strike exploits a memory corruption vulnerability in the Office Web Component (OWC) Spreadsheet ActiveX control.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Outlook Web Components ActiveX Spreadsheet Control Overflow	CWE: 119 CVE: 2009-1534 BID: 35992	This strike exploits a stack overflow with an SEH overwrite in the Outlook Web Components Spreadsheet ActiveX Control. The HTMLURL property is used as the attack vector delivered via HTML/JavaScript code rendered in Internet Explorer.
Strike JScript Scripting Engine Keyword Override Remote Code Execution	CWE: 94 CVE: 2009-1920	This strike exploits a remote code execution vulnerability in the JScript engine. This vulnerability is triggered when a malicious script attempts to override a keyword with a function declaration and then calls the function.
Strike Windows ASF Media File Format Parsing Code Execution (HTTP)	CWE: 94 CVE: 2009-2498	This strike exploits a code execution vulnerability in the Microsoft Windows Media Format Runtime and Windows Media Services file parsing function for Advanced System Format (.ASF/.WMV/.WMA) files.
Strike Windows MP3 Media File Format Parsing Code Execution (HTTP)	CWE: 94 CVE: 2009-2499	This strike exploits a code execution vulnerability in the Microsoft Windows Media Format Runtime and Windows Media Services file parsing function for MP3 files.
Strike Windows Media Player ASF Media File Format Parsing Code Execution (HTTP)	CWE: 119 CVE: 2009-2527	This strike exploits a code execution vulnerability in Microsoft Windows Media Player 6.4 when parsing an Advanced System Format (.ASF/.WMV/.WMA) file containing a Header Extension Object which contains a Index Object with an overly large IndexEntriesCount value.
Strike Windows Media Player ASF Media File Format Header Extension Parsing Code Execution (HTTP)	CWE: 119 CVE: 2009-2527	This strike exploits a code execution vulnerability in Microsoft Windows Media Player 6.4 when parsing an Advanced System Format (.ASF/.WMV/.WMA) file containing a Header Extension Object which contains a Marker Object with an overly large MarkersCount value.
Strike Microsoft Internet Explorer createEventObject propertyName Double Free	CWE: 94 CVE: 2009-2530	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer when creating event objects in javascript.
Strike Microsoft Internet Explorer createEventObject qualifier Double Free	CWE: 94 CVE: 2009-2530	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer when creating event objects in javascript.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer createEventObject srcUrn Double Free	CWE: 94 CVE: 2009-2530	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer when creating event objects in javascript.
Strike Microsoft Internet Explorer createEventObject type Double Free	CWE: 94 CVE: 2009-2530	This strike exploits a memory corruption vulnerability in Microsoft Internet Explorer when creating event objects in javascript.
Strike Microsoft Indexing Service Loop Counter Underwrap	CVE: 2009-2507	This strike exploits a vulnerability in the Microsoft Indexing Service by passing a specially crafted URL to the DecodeURLEscapes() function via an ActiveX control.
Strike Microsoft .NET CLR ArgIterator Stack Pointer Manipulation	CWE: 264 CVE: 2009-0090	This strike uses a web page to instantiate a malicious .NET app that will exploit a flaw in how the .NET CLR implements variable arguments for functions.
Strike GDI+ PNG Integer Overflow Vulnerability (HTTP)	CWE: 189 CVE: 2009-3126	This strike exploits the way the buffer size for the pixel data in interlaced PNGs is calculated by GDI+. The methods used by GDI+ contain integer overflow vulnerabilities.
Strike Microsoft GDI+ WMF Integer Overflow (HTTP)	CWE: 189 CVE: 2009-2500	This strike exploits an arbitrary code execution flaw in the Microsoft GDI+ Rendering Engine for WMF files. This vulnerability is triggered when an overflow integer is passed to an unchecked call to memcpy resulting in a heap-based buffer overflow. Because the flaw is in the underlying GDI+ rendering engine, anything which renders WMF files via GDI+ is affected and vulnerable.
Strike Microsoft Web Services for Devices (WSD) API Stack Buffer Overflow	CWE: 94 CVE: 2009-2512	This strike exploits a vulnerability in the Microsoft Web Services for Devices (WSD) API. The API does not properly handle overly-long Mime-Version header values which allows an attacker to overwrite a single NULL byte on the stack via an overflow of the buffer that the Mime-Version header value is written to.
Strike Microsoft Web Services for Devices (WSD) API Mime-Version Stack Buffer Overflow	CWE: 94 CVE: 2009-2512	This strike exploits a vulnerability in the Microsoft Web Services for Devices (WSD) API. The API does not properly handle overly-long Mime-Version header values which allows an attacker to overwrite a single NULL byte on the stack via an overflow of the buffer that the Mime-Version header value is written to.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Embedded OpenType Font Parser Directory Entry Summed Length & Offset Integer Wrap Code Execution (HTTP)	CWE: 94 CVE: 2009-2514	This strike exploits a vulnerability in Microsoft's Embedded OpenType file parsing engine when parsing an EOT file containing a directory entry where the directory entry's length and offset summed cause an integer wrap. This wrapped integer is then subsequently used to allocate memory for the directory. When the directory data is then written to the allocated buffer, it is overflowed resulting in heap corruption and control of code execution.
Strike Microsoft Office Excel Cache Code Execution (HTTP)	CWE: 94 CVE: 2009-3127	This vulnerability is triggered when Microsoft Excel parses an XLS file which contains a pivot cache stream with an SXDB record with a cfdbdb member value that is larger than the accompanying cfdbTot value. This causes Excel to access memory beyond the bounds of an array, resulting in potential arbitrary code execution. May require user interaction via clicking inside the PivotTable object to produce malicious conditions.
Strike Microsoft Excel Field Sanitization (HTTP)	CWE: 94 CVE: 2009-3134 BID: 36912	Versions of Microsoft Excel prior to the MS09-067 patch contain a vulnerability in which an attacker-controlled value is used to calculate an index into an array, which can lead to arbitrary code execution.
Strike Microsoft Office Word File Information Memory Corruption Vulnerability (HTTP)	CWE: 119 CVE: 2009-3135 BID: 36950	This strike exploits a vulnerability in the way Microsoft Word parses the FIB in Word documents, causing it to copy large amounts of data from the file onto the heap, resulting in possible code execution.
Strike Internet Explorer HTML Object Memory Corruption	CWE: 94 CVE: 2009-3672 BID: 37085	This strike exploits a flaw in Internet Explorer 6 and 7 where objects that were not properly initialized get used, which causes memory corruption and could potentially allow remote attackers to execute arbitrary code.
Strike Microsoft Embedded OpenType Font LZCOMP Decompressor Array Index Overflow Code Execution (HTTP)	BID: 37671 CWE: 189 CVE: 2010-0018	This strike exploits a vulnerability in Microsoft's Embedded OpenType file LZCOMP decompression engine when decompressing a LZX-compressed EOT file where there is the potential for a value used as an array index to overflow, resulting in a read access violation.
Strike Microsoft Internet Explorer HTML Object Use After Free (Aurora)	CWE: 94 CVE: 2010-0248 BID: 37894	This strike exploits a vulnerability in Microsoft Internet Explorer where a pointer to an HTML object can be used even after it has been freed, leading to memory corruption and potentially arbitrary code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft PowerPoint Viewer TextBytes Atom Record Stack Overflow Code Execution (HTTP)	CWE: 119 CVE: 2010-0033	This vulnerability is triggered when PowerPoint attempts to parse a PowerPoint file containing a TextBytes atom with an invalid size value. The unsigned size value read from the file is treated as a signed integer and compared to the signed constant value of 254. This flaw results in the large value being passed to a wrapper to memcpy, which causes an overflow of the stack buffer being written to resulting in stack corruption and potential arbitrary code execution.
Strike Microsoft PowerPoint Viewer TextChars Atom Record Stack Overflow Code Execution (HTTP)	CWE: 119 CVE: 2010-0034	This vulnerability is triggered when PowerPoint attempts to parse a PowerPoint file containing a TextChars atom with an invalid size value. The unsigned size value read from the file is treated as a signed integer and compared to the signed constant value of 254. This flaw results in the large value being passed to a wrapper to memcpy, which causes an overflow of the stack buffer being written to resulting in stack corruption and potential arbitrary code execution.
Strike Microsoft Paint JPEG Integer Overflow Code Execution (HTTP)	CWE: 189 CVE: 2010-0028	This strike transfers a malicious JPG file containing overly-large height and width values. A JPG such as the one described triggers a vulnerability in Microsoft Paint when the application evokes GDI+ to convert the JPG image into a BMP image. Such large height and width values can cause GDI+ to wrap an integer used for memory allocation calculations, resulting in the failure of Paint to reallocate a buffer being written to. Paint will then write data past the end of this buffer, resulting in a write access violation.
Strike Internet Explorer URL Protocol Validation (Command Exec)	CWE: 94 CVE: 2010-0027 BID: 37884	This strike exploits a flaw in Internet Explorer's handling of URL protocol types that leads to bypassing security restrictions.
Strike Internet Explorer URL Protocol Validation (File Access)	CWE: 94 CVE: 2010-0027 BID: 37884	This strike exploits a flaw in Internet Explorer's handling of URL protocol types that leads to bypassing security restrictions.
Strike Microsoft DirectShow AVI Invalid biCrlUsed Value (HTTP)	BID: 38112 CWE: 119 CVE: 2010-0250	This strike triggers a vulnerability when an AVI file containing a video chunk with an invalid biCrlUsed value is used in a GraphEdt.exe AVI/WAVE File Source filter, then that filter's video pin is connected to the input pin of an AVI Splitter filter. NOTE: While the malicious file transferred over the network by this strike is required to trigger the vulnerability, actually triggering the vulnerability requires a considerable amount of user interaction with the malicious file within GraphEdt.exe.
Strike Windows Movie Maker and Producer Buffer Overflow (HTTP)	CWE: 119 CVE: 2010-0265	This strike exploits the way the buffer size for the WmtoolsValid directory structure is allocated. An overly large value will cause an overflow that leads to an application crash and has the potential for code execution. This seems to be related to MS10-016.

Name	References	Description
Strike Microsoft Office Excel Sheet Object Type Confusion Code Execution (BIFF5) (HTTP)	CWE: 94 CVE: 2010-0258	This vulnerability is triggered when Microsoft Excel parses a BIFF5 file that contains ptgArea3d or ptgRef3d BRAI records with an ib (XTI) value of an index into the Worksheet's ExternSheet record's rgXTI array where the XTI structure at that index has either: (a) An encoding value of 2 and the BoundSheet at the same index as the XTI index value in the Worksheet Globals has a dt value greater than 1; or (b) An encoding value other than 2 and the BoundSheet in the Worksheet Globals that matches the name specified in the ExternSheet's rgch value has a dt value greater than 1. The vulnerable code's sanity check on the dt value only verifies that the value is non-zero. By passing an invalid value greater than 1, the sanity check is passed. Later, the pointer to the Chart sheet is re-used as a pointer to a larger Sheet sheet structure, resulting in a read access violation as data is attempted to be read beyond the size of the Chart sheet structure.
Strike Microsoft Office Excel Sheet Object Type Confusion Code Execution (BIFF8) (HTTP)	CWE: 94 CVE: 2010-0258	This vulnerability is triggered when Microsoft Excel parses a BIFF8 file that contains ptgArea3d or ptgRef3d BRAI records with a ptgrgc.PTGWithXTI.ib (XTI) value of an index into the Worksheet Globals ExternSheet record's rgXTI array where the XTI structure at that index has an iTabFirst value of an index into the Worksheet Globals array of BoundSheet records where the record at that index has a dt value greater than 1. The vulnerable code's sanity check on the dt value only verifies that the value is non-zero. By passing an invalid value greater than 1, the sanity check is passed. Later, the pointer to the Chart sheet is re-used as a pointer to a larger Sheet sheet structure, resulting in a read access violation as data is attempted to be read beyond the size of the Chart sheet structure.
Strike Microsoft Internet Explorer Tabular Data ActiveX Control Stack Corruption	BID: 39025 CWE: 94 CVE: 2010-0805	This strike exploits a vulnerability in the Internet Explorer Tabular Data ActiveX control where by an overly-long "DataURL" parameter to the ActiveX control can cause a NULL byte to be written outside the bounds of an array. Arbitrary code execution is possible by controlling where the byte is written on the call stack.
Strike Microsoft Internet Explorer Tabular Data Control ActiveX Memory Corruption	CWE: 94 CVE: 2010-0805 BID: 39025	This strike exploits a vulnerability in the Tabular Data ActiveX control. The way the url is parsed allows an attacker to write a null byte to an unplanned stack address, which may lead to arbitrary code execution.
Strike MPEG Layer-3 Audio Decoder Stack Overflow Vulnerability (HTTP)	CWE: 119 CVE: 2010-0480	This strike exploits a vulnerability in how MPEG Layer-3 (mp3) data is parsed in an AVI file. If a value is present in the nSamplesPerSec field that is not in the case statement used in the parsing code, a stack overflow may occur, leading to possible code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Windows Media Player ActiveX Missing Codec	CVE: 2010-0268 BID: 39351	This strike triggers a vulnerability in the ActiveX control for Windows Media Player 9. The vulnerability is triggered when Windows Media Player 9 attempts to use a stale pointer after attempting to download a missing codec.
Strike Windows Media Player Decompression Vulnerability (HTTP)	CWE: 94 CVE: 2010-1879 BID: 40432	This strike exploits a vulnerability in the way JPEG frames in AVI files are parsed by Windows Media Player. Invalid Huffman table entries can lead to arbitrary code execution.
Strike Microsoft Excel SxView Record Parsing Heap Corruption (HTTP)	CWE: 94 CVE: 2010-1245	This strike exploits an arbitrary program execution flaw in Microsoft Excel 2002. This vulnerability is triggered when a malformed SxView record is parsed in a malicious XLS file.
Strike Microsoft Excel WOPT Record Parsing Vulnerability (HTTP)	BID: 40522 CWE: 94 CVE: 2010-0824	This strike exploits an arbitrary program execution vulnerability within Microsoft Excel 2002, part of the Microsoft Office XP suite. This flaw is triggered when Excel parses a malformed WOPT record in a maliciously crafted XLS file.
Strike Microsoft SharePoint Server 2007 Cross Site Scripting Vulnerability	CWE: 79 CVE: 2010-0817 BID: 39776	Microsoft Sharepoint Server 2007 contains a vulnerability in its "_layouts/help.aspx" page that can allow an attacker to inject his own html into the page via the "cid0" URL parameter and perform a cross-site-scripting attack.
Strike XML Signature HMAC Truncation Authentication Bypass (Server Response)	CVE: 2009-0217 BID: 35671	The specification for including HMAC-SHA1 signatures in XML documents includes a way to specify that only the first 'n' bits of the signature need to be verified. This can be done through the use of the HMACOutputLength tag. XML is commonly used to interact with webservices, many of which utilize this functionality. A client or server can specify a low (one bit being the minimum) HMACOutputLength value, causing the receiving party to verify only HMACOutputLength bits, increasing the chances that the sender will gain unauthorized access to the web service.
Strike Microsoft Access ImexGrid Denial of Service	CWE: 94 CVE: 2010-0814	This strike exploits a vulnerable ActiveX control (ImexGrid.AddColumn()) in Microsoft Access 2003 ACCWIZ.DLL which results in memory corruption and potential code execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Access ImexGrid Denial of Service Variant 2	CWE: 94 CVE: 2010-0814	This strike exploits a vulnerable ActiveX control (ImexGrid.DeleteColumn()) in Microsoft Access 2003 ACCWIZ.DLL which results in memory corruption and potential code execution.
Strike Microsoft Access ImexGrid Denial of Service Variant 3	CWE: 94 CVE: 2010-0814	This strike exploits a vulnerable ActiveX control (ImexGrid.AddColumn()) in Microsoft Access 2003 ACCWIZ.DLL which results in memory corruption and potential code execution.
Strike Microsoft Access ImexGrid Denial of Service Variant 4	CWE: 94 CVE: 2010-0814	This strike exploits a vulnerable ActiveX control (ImexGrid.DeleteColumn()) in Microsoft Access 2003 ACCWIZ.DLL which results in memory corruption and potential code execution.
Strike Internet Explorer Uninitialized Pointer Memory Corruption	CWE: 94 CVE: 2010-2559	This strike triggers a vulnerability in Internet Explorer 8 that causes an uninitialized pointer to be used, which can lead to memory corruption and arbitrary code execution.
Strike Microsoft Cinepak Codec CVDecompress Heap Overflow (HTTP)	CWE: 94 CVE: 2010-2553	This strike exploits an arbitrary program execution flaw in Microsoft Windows (XP,Vista,7) Cinepak Codec CVDecompression routine. This flaw is triggered by incorrect parsing of crafted Cinepak compressed data in a malicious AVI file.
Strike Microsoft Office Excel SXDB Record Parsing Buffer Overflow (HTTP)	CWE: 94 CVE: 2010-2562	This strike exploits a memory corruption vulnerability in Microsoft Excel by forcing Excel to parse a malformed SXDB record in a crafted XLS document, effectively leading to a stack-based buffer overflow and potential code execution conditions. May require user interaction via clicking inside the PivotTable object to produce malicious conditions.
Strike Microsoft Office Uninitialized Memory Corruption (HTTP)	BID: 43706 CWE: 94 CVE: 2010-3329	This strike exploits an arbitrary program execution flaw in Microsoft Office HtmlDlgHelper class caused by uninitialized memory usage and leads to stack memory corruption.
Strike Microsoft Office HtmlDlgHelper Uninitialized Memory Corruption (HTTP)	BID: 43706 CWE: 94 CVE: 2010-3329	This strike exploits an arbitrary program execution flaw in Microsoft Office HtmlDlgHelper class caused by uninitialized memory usage and leads to stack memory corruption.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Windows Media Player Memory Corruption Vulnerability	CWE: 94 CVE: 2010-2745 BID: 43772	This strike exploits a vulnerability the way an html-embedded Windows Media Player (v9-12) de-allocates objects when the page is reloaded.
Strike Wordpad and Windows Shell Com Validation Vulnerability (HTTP)	BID: 40574 CWE: 94 CVE: 2010-1263	This strike attempts to use a blocklisted activex control in an rtf
Strike Microsoft Word RTF Stack Buffer Overflow (HTTP)	BID: 44652 CWE: 119 CVE: 2010-3333	This strike exploits a stack-based overflow vulnerability in the Microsoft Word RTF Parsing Engine and leads to potential code execution.
Strike Internet Explorer CSS Invalid Flag Reference Use After Free	CWE: 399 CVE: 2010-3962 BID: 44536	This strike exploits a heap memory corruption vulnerability present in Microsoft Internet Explorer due to an attempt to access an object that has not been correctly initialized or has been deleted.
Strike Internet Explorer HTML+Time outerText Memory Corruption	CWE: 94 CVE: 2010-3346 BID: 45261	This strike exploits a memory corruption vulnerability present in Microsoft Internet Explorer due to improper handling of the creation and deletion of HTML+TIME elements.
Strike Microsoft OpenType Font Index Vulnerability (HTTP) (Array Index)	CWE: 94 CVE: 2010-3956	This strike exploits a vulnerability in the Windows Open Type Font driver that uses an unchecked offset into an array.
Strike Internet Explorer MSADO CacheSize Integer Overflow	CWE: 20 CVE: 2011-0027 BID: 45698	This strike exploits an integer wrap vulnerability present in the MSADO component of Microsoft Internet Explorer when the CacheSize property of a MSADO recordset object is set to a large size. The vulnerability may allow remote code execution.

Name	References	Description
Strike CreateSizedDIBSection Stack-Based Buffer Overflow (HTTP)	CWE: 119 CVE: 2010-3970 BID: 45662	This strike exploits a stack-based buffer-overflow that occurs when an Office document with a thumbnail that has a negative biClrUsed value is parsed, which can lead to arbitrary code execution.
Strike Internet Explorer Object Management Use After Free	CVE: 2011-1345 BID: 46821	This strike triggers a use-after-free vulnerability present in versions of Internet Explorer prior to the April 2011 updates. This can lead to arbitrary code execution.
Strike Microsoft Internet Explorer 8 Developer Tools ActiveX	CWE: 94 CVE: 2010-0811 BID: 40490	This strike triggers a memory corruption vulnerability in iedvtool.dll (Internet Explorer 8 developer tools) by instantiating an object with clsid 1a6fe369-f28c-4ad9-a3e6-2bcb50807cf1 or 8fe85d00-4647-40b9-87e4-5eb8a52f4759.
Strike Internet Explorer HTTP Redirect Memory Corruption	CWE: 119 CVE: 2011-1262 BID: 48211	This strike exploits a flaw in Microsoft Internet Explorer that is triggered when an HTTP 30x redirect response is received that contains a reference to the CDL protocol in its Location header.
Strike Internet Explorer mshtml!CObjectElement Use After Free	CWE: 119 CVE: 2011-1260 BID: 48208	This strike triggers a use-after-free vulnerability in Microsoft Internet Explorer by generating an html page that contains an invalid object element that is covered by other html elements.
Strike Microsoft Internet Explorer Selection Object Use After Free	CWE: 119 CVE: 2011-1261 BID: 48210	This strike triggers a vulnerability in Internet Explorer by sending a specially crafted html page that contains a style tag using the selection.empty() method. The bug will be triggered if a user clicks anywhere on the page.
Strike Internet Explorer TIME Element Uninitialized Memory	CWE: 119 CVE: 2011-1255 BID: 48206	This strike sends an html page that will cause vulnerable versions of Internet Explorer to use uninitialized memory.

Name	References	Description
Strike Microsoft Internet Explorer VML Use After Free	CWE: 119 CVE: 2011-1266 BID: 48173	This strike triggers a vulnerability in Internet Explorer by sending a specially crafted html page that contains VML (Vector Markup Langauge). Scripts in the html page cause an object to be freed and then again used when the page is being destroyed.
Strike Microsoft Internet Explorer XSLT Memory Corruption	CWE: 119 CVE: 2011-1963 BID: 49037	Microsoft Internet Explorer 7 through 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, aka XSLT Memory Corruption Vulnerability. This strike delivers a payload consistent with triggering the specified vulnerability.
Strike Microsoft Internet Explorer Style Object Memory Corruption	CWE: 119 CVE: 2011-1964 BID: 49039	This strike triggers a vulnerability in Internet Explorer by sending a specially crafted html page that contains a call to the addBehavior method with an invalid parameter on a style object.
Strike Microsoft Corrupted Bitmap Font	CWE: 119 CVE: 2011-2003	This strike exploits a denial of service vulnerability in Microsoft Windows's win32k.sys when viewing a corrupted bitmap font.
Strike Microsoft Internet Explorer Body Element Use-After-Free	CWE: 20 CVE: 2011-2000 BID: 49965	This strike triggers a vulnerability in Internet Explorer by sending a specially crafted html page that contains a call to the clearAttributes method on the body element followed by subsequent references to that element.
Strike Microsoft Internet Explorer VTable Memory Corruption	CWE: 20 CVE: 2011-2001 BID: 49966	This strike triggers a vulnerability in Internet Explorer by sending a specially crafted html page that contains a marquee element with an embedded style tag that is dynamically removed.
Strike Microsoft Internet Explorer HTML Invalid Element Use After Free	CWE: 94 CVE: 2012-0011 BID: 51933	This strike exploits a denial of service vulnerability in Microsoft Internet Explorer when an invalid element is specified and assigned a fixed position, then given focus and subsequently has its position attribute altered.

Name	References	Description
Strike Microsoft SharePoint Server and Foundation 2010 and 2010 SP1 Cross Site Scripting Vulnerability	CWE: 79 CVE: 2012-0145	Microsoft Sharepoint Server and Foundation 2010 and 2010 SP1 contains a vulnerability in its "_layouts/Chart/WebUI/WizardList.aspx" page that can allow an attacker to inject his own code into the page via the "skey" URL parameter and perform a cross-site-scripting attack.
Strike Internet Explorer Col Span Heap Overflow	CWE: 94 CVE: 2012-1876	This strike exploits a heap overflow in Internet Explorer up to and including 10 on Windows 7.
Strike mshtml.dll toStaticHTML Cross Site Scripting	CWE: 200 CVE: 2012-1858	This strike exploits a quote mishandling vulnerability in mshtml.dll which allows to execute dynamic content in otherwise static HTML.
Strike MHTML Cross Site Scripting Vulnerability (image file delivery)	BID: 46055 CWE: 79 CVE: 2011-0096	A cross site scripting vulnerability has been identified in the processing of the MHTML protocol, that allows injection of arbitrary code with no special character requirements. This is an image file delivery where the MHTML is padded at the end of an image file. This does require another exploit to expose the image link in an mhtml format ( mhtml:http://uri/file.ext!action ), this is possible because the MHTML protocol handler ignores the file extension.
Strike Microsoft Video ActiveX Control msvidctl.dll Memory Corruption	CWE: 119 CVE: 2008-0015 BID: 35558	This strike exploits a vulnerability in the Microsoft MSVidCtl ActiveX control when processing a crafted .gif file. This attack has been seen in the wild.
Strike Microsoft Internet Explorer 6.0 Png pngfilt.dll ProcessTRNS() Null Pointer Dereference (HTTP)		Microsoft Internet Explorer 6.0 suffers from a null pointer dereference vulnerability in its parsing of tRNS chunks in a png. If the png is missing the IHDR chunk, a null pointer will be dereferenced leading to denial of service conditions.
Strike Microsoft Visual Studio .NET msdds.dll Remote Code Execution Variant 1	CWE: 119 CVE: 2005-2127 BID: 14594	This strike exploits a buffer overflow in a COM object installed with Microsoft Visual Studio .NET. This strike simulates downloading via HTTP an HTML file that triggers the overflow.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Visual Studio .NET msdds.dll Remote Code Execution Variant 2	CWE: 119 CVE: 2005-2127 BID: 14594	This strike exploits a buffer overflow in a COM object installed with Microsoft Visual Studio .NET. This strike simulates downloading via HTTP an HTML file that triggers the overflow.
Strike Microsoft Windows MSHTA Arbitrary Script Execution - HTTP Download	CVE: 2005-0063 BID: 13132	This strike exploits a flaw in Microsoft Windows that allows non-executable files to be executed. This strike simulates downloading a malicious via HTTP.
Strike Internet Explorer Uninitialized Data Source Memory Corruption	CWE: 94 CVE: 2011-0035 BID: 46157	This strike delivers a payload consistent with triggering a memory corruption flaw in Microsoft Internet Explorer versions 6, 7, and 8. The vulnerability is triggered when erroneously accessing an XML Data Source Object that has not been properly initialized or deleted. This vulnerability, when exploited successfully, may produce remote code execution conditions under the context of the logged-in user, by way of a maliciously crafted HTML document.
Strike Internet Explorer Uninitialized ActiveX Object Memory Corruption	CWE: 94 CVE: 2010-3340 BID: 45255	This strike delivers a payload consistent with triggering a memory corruption flaw in Microsoft Internet Explorer versions 6, 7, and 8. The vulnerability is triggered when erroneously accessing an ActiveX object (specifically an instantiation of the Pkmaxctl.VocabCtl control) that has not been properly initialized or deleted. This vulnerability, when exploited successfully, may produce remote code execution conditions under the context of the logged-in user, by way of a maliciously crafted HTML document.
Strike Internet Explorer Uninitialized HTML Object Memory Corruption	CWE: 94 CVE: 2010-3343	This strike delivers a payload consistent with triggering a memory corruption flaw in Microsoft Internet Explorer versions 6, as embedded in Microsoft Windows 2000, XP, and Server 2003. This vulnerability is triggered by a malicious HTML document crafted causing Internet Explorer to improperly process uninitialized CSS anim objects in memory which can lead to remote control of execution and potential arbitrary code execution. User interaction is required by way of leaving the page either by going to a new unique URL or by simply refreshing the page.
Strike Internet Explorer Uninitialized Object Memory Corruption	CWE: 94 CVE: 2011-0036 BID: 46158	This strike delivers a payload consistent with triggering a memory corruption flaw in Microsoft Internet Explorer versions 6, 7, and 8. The vulnerability is triggered when erroneously accessing an object that has not been properly initialized or deleted. This vulnerability, when exploited successfully, may produce remote code execution conditions under the context of the logged-in user, by way of a maliciously crafted HTML document.
Strike Multiple Browser Marquee Tag Denial of Service	CVE: 2006-2723 BID: 18165	This strike exploits a denial of service (memory corruption) vulnerability that can be used to crash multiple major vendors' web browsers by overflowing the marquee tag.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike MyNewsGroups layersmenu.inc.php myng_root Parameter PHP File Include	CWE: 94 CVE: 2006-3966 BID: 19258	This strike exploits a PHP include flaw in the MyNewsGroups web application.
Strike MySQL Commander dbopen.php home Parameter PHP File Include	BID: 22941 CVE: 2007-1439	This strike exploits a remote file include vulnerability in MySQL Commander
Strike SAP-MySQL MaxDB WebDBM Buffer Overflow	CVE: 2006-4305 BID: 19660	This strike exploits a remote buffer overflow in the SAP/MySQL MaxDB WebDBM management interface
Strike NCTSoft AudFile.dll SetFormatLikeSample ActiveX	BID: 22196 BID: 23892 CWE: 119 CVE: 2007-0018	This strike exploits a flaw in the NCTSoft AudFile.dll ActiveX control when calling the SetFormatLikeSample() function.
Strike IP3 NetAccess getFile.cgi Directory Traversal	CVE: 2007-0883 BID: 22513	This strike exploits a directory traversal flaw in the IP3 NetAccess web server using the getFile.cgi CGI script.
Strike Netscape-iPlanet Search NS-Query-Pat Traversal (Unix)	CVE: 2002-1042 BID: 5191	This strike exploits an directory traversal flaw in search engine provided with the Netscape and iPlanet web servers.
Strike Netscape-iPlanet Search NS-Query-Pat Traversal (Win32)	CVE: 2002-1042 BID: 5191	This strike exploits an directory traversal flaw in search engine provided with the Netscape and iPlanet web servers.
Strike Novell Messenger 2.1 Denial of Service	BID: 52056	This strike causes a denial of service in the Novell Messenger Messaging Agent. The vulnerability is due to failure to verify different data types when processing login messages.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike NoMoKeTos functions_nomoketos_rules.php phpbb_root_path Parameter PHP File Include	BID: 22713  CVE: 2007-1106	This strike exploits a remote PHP include flaw in the NoMoKeTos module.
Strike Novell GroupWise Messenger createsearch memory corruption		This strike exploits a memory corruption vulnerability within Novell GroupWise Messenger. The vulnerability is due to insufficient checking of the type value in the request. A remote attacker may take advantage of this vulnerability to execute the memory corruption attack on the target system.
Strike Novell GroupWise Messenger login memory corruption		This strike exploits a memory corruption vulnerability within Novell GroupWise Messenger. The vulnerability is due to insufficient input checking of the type value in the request. A remote attacker may take advantage of this vulnerability to execute the memory corruption attack on the target system.
Strike Novell GroupWise Messenger HTTP Response Handling Stack Buffer Overflow	CWE: 119  CVE: 2008-2703  BID: 29602	This strike exploits a stack-based buffer overflow present in Novell GroupWise Messenger (GWIM) Client before 2.0.3 HP1 for Windows which allows remote code execution by way of "spoofed server responses" that contain a long string after the NM_A_SZ_TRANSACTION_ID field name.
Strike Novell iPrint Client ActiveX control memory corruption	CWE: 119  CVE: 2011-4185	This strike exploits a memory corruption vulnerability inside the GetPrinterURLList2 function of Novell's iPrint ActiveX control. A user supplied object string rcvs a length validation, and if it is >=512 bytes or the contextName >= 2048 bytes the check fails. The application then proceeds to write stack memory to a different function, which results in invalid memory access.
Strike Novell NetMail WebAdmin Buffer Overflow	BID: 22857  CVE: 2007-1350	This strike exploits a remote stack overflow in the Novell NetMail WebAdmin component's HTTP interface by providing an overly-long Basic Authentication username.
Strike Novell ZENworks Mobile Management Cross-Site Scripting (XSS) Vulnerability		This strike exploits a cross-site scripting (XSS) vulnerability in Novell ZENworks Mobile Management. The vulnerability is due to improper validation while processing HTTP requests with username and domain parameters. An attacker could exploit this vulnerability in order to run malicious scripts on the target machine.
Strike Nullsoft Shoutcast Server Request Log Cross-Site Scripting	CWE: 79  CVE: 2007-1229  BID: 22742	This strike exploits a cross-site scripting vulnerability in the Nullsoft Shoutcast log viewer web interface

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike OABOARD Web Forum forum.php inc Parameter PHP File Include	CVE: 2006-0076  BID: 16105	This strike exploits a PHP include flaw in the OABoard Forum.
Strike Alcatel OmniPCX Office FastJSData.cgi id2 Parameter Command Execution	CWE: 20  CVE: 2008-1331  BID: 28758	This strike exploits an arbitrary command execution flaw the Alcatel OmniPCX Office web interface. This flaw can be triggered by inserting shell metacharacters into the id1 or id2 parameters of the FastJSData.cgi web application.
Strike Alcatel OmniPCX Office MasterCGI user Parameter Command Execution	CWE: 20  CVE: 2007-3010  BID: 25694	This strike exploits an arbitrary command execution flaw the Alcatel OmniPCX Office web interface. This flaw can be triggered by inserting shell metacharacters into the user parameter of the MasterCGI web application.
Strike Open Educational System CONF_CONFIG_PAT H Parameter PHP File Include Vulnerability	BID: 22858  CVE: 2007-1372	This strike exploits a remote file include vulnerability in Open Educational System
Strike OPENi-CMS Plugin index.php oi_dir Parameter PHP File Include	CVE: 2007-0881  BID: 22511	This strike exploits a PHP include flaw in the OPENi-CMS web application.
Strike OpenView connectedNodes.ov pl node Parameter Command Execution	BID: 14662  CVE: 2005-2773	This strike exploits an arbitrary command execution flaw the OpenView connectedNodes.ovpl CGI application.
Strike Opera JavaScript Alert() Buffer Overflow		This strike exploits a flaw in Opera 10.10 in which overly long values given to the JavaScript Alert() function can cause the browser to crash
Strike Opera 10.53 JavaScript getImageData() Memory Corruption DoS		This strike exploits a flaw in Opera 10.53 in which a malformed call to the JavaScript getImageData() function can cause the browser to crash.
Strike Opera SVG Animation Element Denial of Service		This strike exploits a flaw in the way Opera v10.63 handles malformed SVG animation elements which results in the browser window crashing.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle Application Server BPEL Module Linked XSS	CVE: 2008-4014 BID: 33177	This strike exploits a cross-site scripting vulnerability in the Oracle Application Server BPEL Module. An attacker may append a persistent, malicious script fragment to the end of a normal URL request.
Strike Oracle Data Quality LoaderWizard Type Confusion		This strike exploits an Oracle Data Quality LoaderWizard vulnerability which is due to absence of input validation in the DataPreview method. An attacker could exploit this vulnerability in order to remotely execute malicious code.
Strike Oracle 9iAS Dynamic Monitoring Services Anonymous Access Variant 2	CWE: 287  CVE: 2002-0563  BID: 4293	This strike exploits a default configuration flaw in the Oracle 9i Application Server version 1.0.2.x.
Strike Oracle 9iAS Dynamic Monitoring Services Anonymous Access Variant 11	CWE: 287  CVE: 2002-0563  BID: 4293	This strike exploits a default configuration flaw in the Oracle 9i Application Server version 1.0.2.x.
Strike Oracle 9iAS Dynamic Monitoring Services Anonymous Access Variant 12	CWE: 287  CVE: 2002-0563  BID: 4293	This strike exploits a default configuration flaw in the Oracle 9i Application Server version 1.0.2.x.
Strike Oracle 9iAS Dynamic Monitoring Services Anonymous Access Variant 3	CWE: 287  CVE: 2002-0563  BID: 4293	This strike exploits a default configuration flaw in the Oracle 9i Application Server version 1.0.2.x.
Strike Oracle 9iAS Dynamic Monitoring Services Anonymous Access Variant 4	CWE: 287  CVE: 2002-0563  BID: 4293	This strike exploits a default configuration flaw in the Oracle 9i Application Server version 1.0.2.x.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle 9iAS Dynamic Monitoring Services Anonymous Access Variant 5	CWE: 287 CVE: 2002-0563 BID: 4293	This strike exploits a default configuration flaw in the Oracle 9i Application Server version 1.0.2.x.
Strike Oracle 9iAS Dynamic Monitoring Services Anonymous Access Variant 6	CWE: 287 CVE: 2002-0563 BID: 4293	This strike exploits a default configuration flaw in the Oracle 9i Application Server version 1.0.2.x.
Strike Oracle 9iAS Dynamic Monitoring Services Anonymous Access Variant 7	CWE: 287 CVE: 2002-0563 BID: 4293	This strike exploits a default configuration flaw in the Oracle 9i Application Server version 1.0.2.x.
Strike Oracle 9iAS Dynamic Monitoring Services Anonymous Access Variant 8	CWE: 287 CVE: 2002-0563 BID: 4293	This strike exploits a default configuration flaw in the Oracle 9i Application Server version 1.0.2.x.
Strike Oracle 9iAS Dynamic Monitoring Services Anonymous Access Variant 10	CWE: 287 CVE: 2002-0563 BID: 4293	This strike exploits a default configuration flaw in the Oracle 9i Application Server version 1.0.2.x.
Strike Oracle FlashTunnelService Deletion of Arbitrary Files		This strike exploits a vulnerability in Oracle's Business Transaction Management FlashTunnelService where an arbitrary file may be deleted from the system. Note that this service may be configured to run on different ports.
Strike Oracle GlassFish Directory Traversal		This strike exploits a directory traversal vulnerability in Oracle GlassFish 4.1 and prior versions. The vulnerability can be exploited by issuing a crafted HTTP GET request utilizing a %C0%2F instead of (/), URL encoding. The vulnerability allows attackers to read arbitrary files on the server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Oracle HTTP Server username XSS Vulnerability	BID: 9484 CVE: 2004-2115	This strike exploits an XSS vulnerability in the Oracle HTTP Server (based on Apache)
Strike Oracle HTTP Server password XSS Vulnerability	BID: 9484 CVE: 2004-2115	This strike exploits an XSS vulnerability in the Oracle HTTP Server (based on Apache)
Strike Oracle HTTP Server action XSS Vulnerability	BID: 9484 CVE: 2004-2115	This strike exploits an XSS vulnerability in the Oracle HTTP Server (based on Apache)
Strike Oracle Java 5,6,7 ZipFile readCEN Denial of Service	BID: 52013 CVE: 2012-0501	This strike exploits an denial of service vulnerability in Oracle Java. The vulnerability is due to a recursion error in the Oracle Java ZipFile class when a malicious zipfile is processed.
Strike Oracle VM ovs-agent XML-RPC Remote Command Injection	CVE: 2010-3582 BID: 44031	This strike exploits an input sanitization flaw in the XML-RPC interface of the Oracle Virtual Server Agent. The flaw exists in the utl_test_url function and allows an attacker to execute arbitrary commands on the server.
Strike Oracle Secure Backup exec_qr() \$ora_osb_bgcookie Command Execution	CVE: 2008-5448 BID: 33177	This strike sends a command execution attack leveraging an unsanitized variable used by Oracle Secure Backup's exec_qr() function.
Strike Oracle Secure Backup exec_qr() \$ora_osb_lcookie Command Execution	CVE: 2008-5448 BID: 33177	This strike sends a command execution attack leveraging an unsanitized variable used by Oracle Secure Backup's exec_qr() function.
Strike Oracle Secure Backups exec_qr() \$rbtool Command Execution	CVE: 2008-5448 BID: 33177	This strike sends a command execution attack leveraging an unsanitized variable used by Oracle Secure Backup's exec_qr() function.
Strike Oracle TimesTen Data Server Log Format String	CVE: 2008-5440 BID: 33177	This strike exploits a format string vulnerability Oracle Database 7.0.5's TimesTen Data Server. An attacker may send a format string to the event viewer, causing the component to either crash or execute malicious code.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike osCommerce 2.3.4.1 - Remote Code Execution	EXPLOITDB : 44374	This strike exploits a code execution vulnerability in osCommerce 2.3.4.1. This vulnerability is due to improper sanitization of the HTTP data when the client sends http traffic to the server. A remote attacker can trigger this vulnerability by sending a malicious request to the web interface. This results in the ability to execute system commands on the target device.
Strike ManageEngine DesktopCentral AgentLogUpload Arbitrary File Upload	BID: 63784 CVE: 2013-7390	This strike exploits a vulnerability in ManageEngine DesktopCentral software suite. Due to improper authorization, a remote authenticated attacker may upload an arbitrary files through the AgentLogUpload servlet. All versions of the software prior to 8.0.0 build 80293 are vulnerable.
Strike Mozilla Firefox xul.dll Large Window Handling Null Pointer Deference DOS Weakness	BID: 67501	This strike exploits a vulnerability inside the Mozilla Firefox Web Browser. Specifically, it targets a flaw in how the xul.dll library handles overly large windows. If a user accesses a specially crafted page, an application crash may be triggered leading to a DOS condition. All versions of Firefox prior to 29.0.1 are vulnerable to this attack.
Strike SolarWinds Storage Manager AuthenticationFilter Authentication Bypass	BID: 69438	This strike exploits a vulnerability inside SolarWinds Storage Manager which allows bypass of authentication filters. This in turn can lead to arbitrary file upload and code execution on the target server.
Strike ActualScript ActualAnalyzer aa.php Cookie Command Execution		This strike exploits a command execution vulnerability in ActualScript ActualAnalyzer. An HTTP request with a specially crafted cookie value can be used to execute arbitrary commands with user privileges on the target machine.
Strike Wordpress MailChimp Subscribe Forms PHP Code execution		This strike exploits a PHP code execution vulnerability in Wordpress plugin MailChimp Subscribe Form. The vulnerability is due to insufficient validation of sm_email and sm_name HTTP request parameters. A malicious attacker can exploit this by inserting PHP code to the parameters in HTTP requests.
Strike WebUI mainfile.php arbitrary command injection		This strike exploits a command injection vulnerability in WebUI. The vulnerability is due to improper validation of user supplied data in mainfile.php. By exploiting this vulnerability, an unauthenticated attacker can execute arbitrary code on the target system.
Strike ManageEngine Desktop Central MSP FileUploadServlet arbitrary file upload		This strike exploits a file upload vulnerability in multiple ManageEngine products. The vulnerability is due to improper sanitization of user supplied HTTP parameters in FileUploadServlet. An unauthenticated attacker can exploit this vulnerability by sending a specially crafted HTTP request to the vulnerable server leading to arbitrary code execution.
Strike ManageEngine Applications Manager CommonAPIUtil SyncMonitors SQL Injection		This strike exploits an SQL injection vulnerability in ManageEngine Application Manager. The vulnerability is due to improper validation of user supplied input in the SyncMonitors method. An unauthenticated attacker can exploit this vulnerability by sending crafted HTTP requests to the vulnerable server.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Internet Explorer CTxtPtr moveEnd Negative Value Memory Access		This strike exploits a memory access vulnerability in Microsoft Internet Explorer. A TextRange element in the DOM tree of a specially crafted HTML page can be manipulated in such a way as to trigger memory reading outside the defined buffer. Successful exploitation can result in disclosure of random heap data or abnormal termination of Internet Explorer.
Strike Sybase M-Business Anywhere agSoap.exe Closing Tag Buffer Overflow	BID: 47775	This strike exploits a heap buffer overflow vulnerability in Sybase M-Business Anywhere. The vulnerability is due to insufficient validation of SOAP requests sent to the service interface. By specially crafting a malicious SOAP request, an unauthenticated attacker could execute arbitrary commands on the server.
Strike CA Total Defense Suite UNC Management SQL Injection		This strike exploits a SQL injection vulnerability within CA Total Defense Suite. This vulnerability is due to improper sanitation of parameters in a procedure. A remote attacker can take advantage of this vulnerability to inject SQL commands.
Strike EGallery PHP File Upload Vulnerability	BID: 54464	This strike exploits a vulnerability in EGallery. The vulnerability allows unauthenticated file uploads which can result in arbitrary code execution.
Strike Sinapsi eSolar Light Photovoltaic System Monitor Command Injection	BID: 55872  CWE: 264  CVE: 2012-5863	This strike exploits a command injection vulnerability in Sinapsi eSolar Light Photovoltaic System Monitor.
Strike D-Link DIR-605L Captcha Handling Buffer Overflow	BID: 56330	This strike exploits a buffer overflow vulnerability inside D-Link DIR-605L devices that can lead to remote code execution. The vulnerability is present inside the FILECODE parameter sent through http requests.
Strike D-Link Devices Command.php Unauthenticated Remote Command Execution	BID: 57734	This strike exploits an unauthenticated remote command execution vulnerability that is present on several D-Link devices. The attack is performed through the command.php script.
Strike SAP NetWeaver Portal ConfigServlet Remote Command Execution		This strike exploits a vulnerability in SAP NetWeaver Portal, more specifically how input is handled by the ConfigServlet. Due to improper authorization, a remote unauthenticated attacker may execute system commands using the system privileges associated with the NetWeaver process. All versions of the software prior to 7.01 are vulnerable.
Strike HP LaserJet Pro Webadmin Password reset		This strike exploits a vulnerability in the HP LaserJet Pro printer. Due to improper validations a remote attacker may change the password of a webadmin to an arbitrary value. The P1606dn model printers are vulnerable to this attack.
Strike PineApp Mail-SeCure livelog.html Multiple Command Execution		This strike exploits an arbitrary command execution vulnerability in PineApp Mail-SeCure. A specially crafted HTTP request can be sent to livelog.html to execute arbitrary commands with root privileges.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike PineApp Mail-SeCure conflivelog.pl Command Execution		This strike exploits an arbitrary code execution vulnerability in PineApp Mail-SeCure. A specially crafted HTTP request can be sent to conflivelog.pl to execute arbitrary commands with privileges of the qmailq user.
Strike PineApp Mail-SeCure test_li_connection.php iptest Command Execution	CWE: 94 CVE: 2013-6829	This strike exploits an arbitrary code execution vulnerability in PineApp Mail-SeCure. A specially crafted HTTP request can be sent to test_li_connection.php to execute arbitrary commands with root privileges.
Strike PineApp Mail-SeCure confpremenu.php export logs Command Execution		This strike exploits an arbitrary code execution vulnerability in PineApp Mail-SeCure. A specially crafted HTTP request can be sent to confpremenu.php to execute arbitrary commands with privileges of the qmailq user.
Strike PineApp Mail-SeCure confpremenu.php Command Execution		This strike exploits an arbitrary code execution vulnerability in PineApp Mail-SeCure. A specially crafted HTTP request can be sent to confpremenu.php to execute arbitrary commands with privileges of the qmailq user.
Strike Mitsubishi MCWorkX ActiveX Control File Execution	CWE: 94 CVE: 2013-2817 BID: 62414	This strike exploits a Mitsubishi MCWorkX ActiveX control code execution vulnerability which is due to no confirmation when executing the command in the ActiveX control. Remote attackers may do arbitrary file creation on the target system.
Strike Nagios Core Config Manager tfPassword SQL Injection		This strike exploits an authentication bypass vulnerability that is accessible via SQL injection inside of Nagios Config Manager
Strike Apple OS X CFNetwork HTTP 302 Status Denial of Service	BID: 22249  BID: 26444  CWE: 119  CVE: 2007-0464	Apple's Mac OS X Core Foundation is vulnerable to a denial of service in CFNetwork when processing HTTP 302 and 301 messages with a non-existent Location: header.
Strike Mac OS X Finder DMG Volume Name Memory Corruption (HTTP)	BID: 21980  CWE: 119  CVE: 2007-0197	This transfers a malicious disk image (DMG) file to a Mac OS X target.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Flip4Mac Memory Corruption (HTTP)	BID: 22286 CVE: 2007-0466	This strike exploits a memory corruption flaw in Telestream Flip4Mac when handling WMF files.
Strike Apple OS X QuickDraw GetSrcBits32ARGB Memory Corruption Denial of Service (HTTP)	BID: 22207 CVE: 2007-0462	This strike exploits a denial of service condition in Apple's Mac OS X when opening a malformed PICT file.
Strike Apple OS X Safari Format String	CVE: 2007-0644 BID: 22326	Safari on Apple's Mac OS X is vulnerable to a format string vulnerability in a call to window.console.log().
Strike Mac OS X Safari x-man-page URI Terminal Escape Command Execution	CVE: 2005-1342 BID: 13502	This strike exploits a flaw in the x-man-page URI handler in the Safari web browser.
Strike PDF Launch Action Feature Adobe Fix Bypass (HTTP)	CWE: 264 CVE: 2010-1240 BID: 39109	This strike bypasses the fix Adobe made for the original PDF Launch Action vuln ( <a href="http://blog.didierstevens.com/2010/03/29/escape-from-pdf/">http://blog.didierstevens.com/2010/03/29/escape-from-pdf/</a> , strikeids E10-3yg00 - E10-3yg07.) Adobe's fix maintained a blocklist of dangerous extensions in the registry (.exe, .bat, etc.) This is bypassed by adding one or two sets of double quotes around the file, which adds one or two quotes onto the end of the parsed extension (.exe != .exe "")
Strike PDF Launch Action Feature (HTTP)	CWE: 264 CVE: 2010-1240	The PDF file format has a feature that allows an external program to be run (the "/Launch" action). An attacker can create a PDF that makes use of this feature to execute programs on the client's computer.
Strike Pegasus Imaging ImagXpress ActiveX File Delete	CWE: 22 CVE: 2007-5320 BID: 25949	This strike exploits an ActiveX bug in Pegasus Imaging ImagXpress that allows arbitrary files to be deleted.
Strike Pegasus Imaging ImagXpress ActiveX File Overwrite	CWE: 22 CVE: 2007-5320 BID: 25948	This strike exploits an ActiveX bug in Pegasus Imaging ImagXpress that allows arbitrary files to be overwritten.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike ESF pfSense 2.2.6 Command Injection	EXPLOITDB : 39709	This strike exploits a vulnerability in ESF pfSense 2.2.6. Specifically, status_rrd_graph_img.php does not properly validate the graph parameter. Certain characters are able to escape the filter and allow for a shell command to be built and executed. This is an authenticated attack, however, a remote attacker could leverage a CSRF vulnerability by enticing an authenticated victim to execute this code allowing for command execution with that user's current privileges.
Strike PHF Qname Parameter Command Execution	BID: 629 CVE: 1999-0067	This strike exploits an arbitrary command execution flaw the 'phf CGI application.
Strike Philboard philboard_forum.asp forumid Parameter SQL Injection	CVE: 2007-0920 BID: 22532	This strike exploits a SQL injection flaw in the Philboard web application.
Strike Phorecast index.php include Parameter PHP File Include	CVE: 2001-1049 BID: 3388	This strike exploits a PHP include flaw in the Phorecast web application.
Strike Phorecast index.php include dir Parameter PHP File Include	CVE: 2001-1049 BID: 3388	This strike exploits a PHP include flaw in the Phorecast web application.
Strike Phormation PHP Library index.php include Parameter PHP File Include	CVE: 2001-1237 BID: 3393	This strike exploits a PHP include flaw in the Phormation PHP Library.
Strike PHP5 Hash Collision Denial Of Service	CWE: 20 CVE: 2011-4885 BID: 51193	This strike exploits a denial of service bug in PHP5 when parameters have the same internal hash.
Strike phpSecurePages secure.php cfgProgDir Parameter PHP File Include	CVE: 2001-1468 BID: 2970	This strike exploits a PHP include flaw in the phpSecurePages web authentication application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike PHP5 php_register_variable_ex Buffer Overflow	CWE: 399  CVE: 2012-0830  BID: 51830	This strike exploits a denial of service bug in PHP 5.3.9 and any back-patched versions, that was introduced as a fix for CVE-2011-4885. It exploits an error condition in php_register_variable_ex when the number of post variables exceeds max_input_vars.
Strike PHPAuction view.inc.php phpAds_path Parameter PHP File Include	CVE: 2006-3984  BID: 19254	This strike exploits a PHP remote file include flaw in PHPAuction.
Strike PHP DateTimeZone Object Unserialize Type Confusion		This strike exploits a vulnerability in PHP which is triggered when trying to deserialize a serialized DateTimeZone object. The vulnerability can be exploited through user supplied parameters which are then passed to the vulnerable function. If exploited the vulnerability can result in remote code execution under the context of the service running the PHP server.
Strike PHP Exif Integer Overflow Denial of Service	CWE: 189  CVE: 2011-4566  BID: 50907	This strike targets a vulnerability in the PHP Exif metadata parser. The vulnerability is due to failure to account for integer overflow when parsing Image File Directory (IFD) entries. If the target system is configured to automatically parse uploaded image files, an unauthenticated attacker could upload a malicious file in order to trigger a Denial of Service condition.
Strike PHP Generic MembreManager.php include_path Parameter PHP File Include	CVE: 2007-0584  BID: 22287	This strike exploits a PHP remote file include vulnerability in the PHP Generic MembreManager web application.
Strike PHP Nuke Blind SQL Injection	BID: 22638  CVE: 2007-1061	This strike exploits a blind SQL injection vulnerability in the PHP Nuke CMS
Strike PHP POST File Upload PHP GLOBALS Variable Overwrite	CVE: 2005-3390  BID: 15250	This strike exploits a vulnerability in PHP which allows an attacker to overwrite the PHP \$GLOBALS variable when performing a POST operation with a multipart/form-data request.
Strike PHP POST File Upload Overflow	CVE: 2002-0081  BID: 4183	This strike exploits a remote heap overflow in the PHP programming language function php_mime_split.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike PHP zip --URL Wrapper Buffer Overflow (HTTP)	CVE: 2007-1339  BID: 22883	This strike exploits a buffer overflow in the 'zip://' protocol handler of PHP's fopen and similar functions
Strike PHP Ads new helperfunction.php include Parameter PHP File Include	CVE: 2001-1054  BID: 3392	This strike exploits a PHP include flaw in the PHPAdsNew web application.
Strike PHP Ads new helperfunction.php include_dir Parameter PHP File Include	CVE: 2001-1054  BID: 3392	This strike exploits a PHP include flaw in the PHPAdsNew web application.
Strike phpBB highlight Parameter Remote Code Execution Variant 1	CVE: 2005-2086  CVE: 2004-1315  BID: 14086  BID: 10701	This strike exploits a command execution flaw in phpBB, a web forums application.
Strike phpBB highlight Parameter Remote Code Execution Variant 2	CVE: 2005-2086  CVE: 2004-1315  BID: 14086  BID: 10701	This strike exploits a command execution flaw in phpBB, a web forums application.
Strike PHPenpals profile.php personalID Parameter SQL Injection	CWE: 89  CVE: 2006-0074  BID: 16109	This strike exploits a SQL injection flaw in the Jevontech PHPenpals script.
Strike phpFileManager Command Execution Vulnerability Through cmd Parameter	EXPLOITDB : 37709	This strike exploits a remote command execution vulnerability in phpFileManager. The vulnerability is due to improper filtering of HTTP cmd and action parameters. An attacker could exploit this vulnerability in order get code execution on the target machine.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike PHPLiveHelper global.php abs_path Parameter PHP File Include	CVE: 2006-4051  BID: 19349	This strike exploits a PHP include flaw in the PHP Live Helper web application (global.php).
Strike PHP Live Helper help.php css_path Parameter PHP File Include	BID: 19116	This strike exploits a PHP include flaw in the Live Helper web application.
Strike phpMyAdmin sql.php goto Parameter PHP File Include	CVE: 2001-0478  BID: 2642	This strike exploits a PHP include vulnerability in phpMyAdmin 2.1.0.
Strike phpMyAdmin tbl_replace.php goto Parameter PHP File Include	CVE: 2001-0478  BID: 2642	This strike exploits a PHP include vulnerability in phpMyAdmin 2.1.0.
Strike PHPSimpleShop index.php abs_path Parameter PHP File Include	CVE: 2006-4052  BID: 19382	This strike exploits a PHP include flaw in the PHP Simple Shop web application (admin/index.php).
Strike PHPSimpleShop adminindex.php abs_path Parameter PHP File Include	CVE: 2006-4052  BID: 19382	This strike exploits a PHP include flaw in the PHP Simple Shop web application (admin/adminindex.php).
Strike PHPSimpleShop adminglobal.php abs_path Parameter PHP File Include	CVE: 2006-4052  BID: 19382	This strike exploits a PHP include flaw in the PHP Simple Shop web application (admin/adminglobal.php).
Strike PHPSimpleShop login.php abs_path Parameter PHP File Include	CVE: 2006-4052  BID: 19382	This strike exploits a PHP include flaw in the PHP Simple Shop web application (admin/login.php).
Strike PHPSimpleShop menu.php abs_path Parameter PHP File Include	CVE: 2006-4052  BID: 19382	This strike exploits a PHP include flaw in the PHP Simple Shop web application (admin/menu.php).

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike PHPSimpleShop header.php abs_path Parameter PHP File Include	CVE: 2006-4052  BID: 19382	This strike exploits a PHP include flaw in the PHP Simple Shop web application (admin/header.php).
Strike PollMentor pollmentorres.asp id Parameter SQL Injection	BID: 22542  CWE: 89  CVE: 2007-0984	This strike exploits an SQL injection vulnerability in PollMentor 2.0
Strike Microsoft Powerpoint 2003 Heap Overflow (HTTP)		This strike exploits a heap overflow vulnerability in Microsoft Office 2005 Powerpoint
Strike pSlash Web Portal index.php include_dir Parameter PHP File Include	CVE: 2001-1235  BID: 3395	This strike exploits a PHP include flaw in the pSlash web portal application.
Strike Apple QTJava toQTPointer() Arbitrary Memory Access (QTBurn)	CVE: 2007-2175  BID: 23608	This strike exploits an arbitrary memory access vulnerability in the QTJava library using a malicious Java applet.
Strike Quicktime rstp --Handler Buffer Overflow	CVE: 2007-0015  BID: 21829	This strike exploits a buffer overflow vulnerability in Apple Quicktime. This exploit simulates a download of the exploit over HTTP on port 80.
Strike Apple Quicktime SMIL Integer Overflow Exploit	CVE: 2007-2394  BID: 24873	This strike exploits a flaw in Quicktime's handing of invalid SMIL files when loaded in a browser.
Strike raSMP index.php record_hit() Function User-Agent XSS	CVE: 2006-0084  BID: 16138	This strike exploits a cross site scripting flaw in the raSMP web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike RealPlayer rmoc3260.dll ActiveX Control Remote Code Execution	CWE: 399 CVE: 2008-1309 BID: 28157	This strike exploits a code execution vulnerability in the RealPlayer rmoc3260.dll ActiveX control.
Strike Redaxo CMS Addon MyEvents 2.2.1 - SQL Injection	EXPLOITDB : 44261	This strike exploits a SQL injection vulnerability in the Redaxo CMS Addon MyEvents. This vulnerability is due to improper sanitization for the parameter "myevents_id". A remote attacker can access backend contents with successful exploitation.
Strike Microsoft IIS RSA SecurID Web Agent Overflow	CVE: 2005-1471 BID: 13524	This strike exploits a heap overflow bug in the RSA SecurID Web Agent which runs on IIS.
Strike Sabdrimer advanced1.php pluginpath[0] Parameter CMS PHP File Include	CVE: 2006-3520 BID: 18907	This strike exploits a PHP include flaw in the Sabdrimer CMS web application.
Strike Safari iframe Remote Code Execution-Denial of Service	CWE: 20 CVE: 2011-5046 BID: 51122	This strike exploits a memory corruption vulnerability in Windows 7 x64 win32k.sys via Apple Safari. Other Webkit browsers may be vulnerable too. The flaw occurs when handling crafted height values for OS skinned elements, such as iframes and buttons.
Strike Safari Use-After-Free Parent.Close() Vulnerability	CWE: 399 CVE: 2010-1939 BID: 39990	Safari 4.0.5 and 4.0.4 are vulnerable to a use-after-free exploit that can lead to code execution. Other versions (4.0.X versions prior to 4.0.4) are at least susceptible to denial of service attacks via the same vector. The vulnerability is triggered when a child window stores a reference to its parent, attempts to close the parent, and then tries to access a property/call a function on the parent.
Strike Safari XSLT Arbitrary File Creation	CWE: 20 CVE: 2011-1774 BID: 48840	This strike an arbitrary file creation in Safari due to a specially crafted XSLT transformation. Versions prior to 5.0.6 are affected.
Strike Best Software SalesLogix Authentication Bypass	CVE: 2004-1612 BID: 11450	This strike sends a malicious cookie value that will cause the SalesLogix software to admit administrator access

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Best Software SalesLogix view id Parameter SQL Injection	CVE: 2004-1612 BID: 11450	This strike exploits an SQL injection vulnerability in SalesLogix
Strike Samsung SmartViewer CNC_Ctrl ActiveX Control Remote Code Execution	BID: 77084 CWE: 20 CVE: 2015-8040	This strike exploits an out of bounds indexing vulnerability in Samsung SmartViewer CNC_Ctrl ActiveX. The flaw is due to insufficient validation of input to the rtsp_getdlsendtime method by the CNC_Ctrl ActiveX control. By enticing a user to visit a malicious web page, arbitrary code can be executed on the client system.
Strike SAP GUI TabOne Caption Buffer Overflow	CWE: 119 CVE: 2008-4827 BID: 33148	This strike exploits a buffer overflow vulnerability present in the SizerOne ActiveX library loaded by the SAP GUI. Due to an issue involving improper bounds-checking, a malicious web page can cause the AddTab function to generate a tab caption that is too large for the buffer to hold, leading to system instability and the possibility of remote code execution.
Strike SAP Internet Transaction Server Directory Traversal	CVE: 2003-0748 BID: 8516	This strike exploits an directory traversal flaw in the SAP Internet Transaction Server.
Strike SAP Internet Transaction Server wgate.dll ~service Parameter XSS	CVE: 2003-0749 BID: 8517	This strike exploits a cross-site scripting flaw in the SAP Internet Transaction Server
Strike SAP Message Server Server Group Parameter Overflow	CVE: 2007-3624 BID: 24765	This strike exploits a buffer overflow in the SAP Message Server.
Strike SaPHPLesson add.php forumid Parameter SQL Injection	CVE: 2006-2835 BID: 18934	This strike exploits an SQL injection flaw in the SaPHPLesson web application.
Strike SaPHPLesson show.php lessid Parameter SQL Injection	CVE: 2006-2835 BID: 18934	This strike exploits an SQL injection flaw in the SaPHPLesson web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike SaveWeb Portal 3.4 menu_dx.php SITE_Path Parameter PHP File Include	CVE: 2005-2687 CVE: 2006-4012 BID: 19306	This strike exploits a PHP remote file include flaw in the SaveWeb Portal 3.4 web application (menu_dx.php).
Strike SaveWeb Portal 3.4 poll.php SITE_Path Parameter PHP File Include	CVE: 2005-2687 CVE: 2006-4012 BID: 19306	This strike exploits a PHP remote file include flaw in the SaveWeb Portal 3.4 web application (poll.php).
Strike SaveWeb Portal 3.4 view_polls.php SITE_Path Parameter PHP File Include	CVE: 2005-2687 CVE: 2006-4012 BID: 19306	This strike exploits a PHP remote file include flaw in the SaveWeb Portal 3.4 web application (view_polls.php).
Strike ScozBook auth.php adminname Parameter SQL Injection	CVE: 2006-0079 BID: 16115	This strike exploits a SQL injection flaw in the ScozBook web application.
Strike Serendipity Unauthenticated SQL Injection	CVE: 2007-1326 BID: 22774	This strike exploits an SQL injection vulnerability in the Serendipity Weblog package
Strike Microsoft IIS ServerVariables_JScript.asp Information Disclosure		This strike attempts to access a sample script included with IIS 4.0 that is vulnerable to a physical path disclosure issue.
Strike Microsoft Sharepoint 2007 Path Info XSS	BID: 23832 CWE: 79 CVE: 2007-2581	This strike triggers a cross-site scripting vulnerability in the Microsoft Sharepoint 2007 web service.

Name	References	Description
Strike Windows Shortcut Font Name Overflow (HTTP)	CVE: 2005-2118 CVE: 2005-0550 BID: 15070 BID: 13115	This strike exploits two different vulnerabilities in the Windows operating system. The first flaw triggers a stack overflow in the CSRSS process when a malformed shortcut is opened. The second flaw triggers a stack overflow in Windows Explorer when the properties of a malformed shortcut file are viewed.
Strike Site-Assistant menu.php paths[version] Parameter PHP File Include	CVE: 2007-0867 BID: 22467	This strike exploits a PHP include flaw in the Site-Assistant web application.
Strike Skype URI Handler Input Validation Vulnerability	BID: 38699	This strike exploits a vulnerability in the way Skype parses skype-protocol urls, such as skype:user123?call. The vulnerability allows an attacker to pass additional command-line arguments to the Skype executable, which may force the user to persist his/her credentials in a remote location, such as an UNC share.
Strike Microsoft Office Smart Tag Code Execution (http) Variant 1	BID: 18037 CVE: 2006-2492	This strike exploits an arbitrary code execution flaw in Microsoft Office, using the "Smart Tag" feature.
Strike Microsoft Office Smart Tag Code Execution (http) Variant 2	BID: 18037 CVE: 2006-2492	This strike exploits an arbitrary code execution flaw in Microsoft Office, using the "Smart Tag" feature.
Strike SMF Forum smf.php mosConfig_absolute_path Parameter PHP File Include	CWE: 94 CVE: 2006-3773 BID: 18924	This strike exploits a PHP include flaw in the Mambo SMF Forum web application.
Strike SolusLabs SolusVM centralbackup.php SQL injection arbitrary command execution		This strike exploits a SQL injection vulnerability with arbitrary command execution in SolusVM. A specially crafted POST request can be sent to an active VM, resulting in arbitrary command execution.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike SQuery ase.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery halo.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery hlife.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery hlife2.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery igi2.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery main.lib.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery netpanzer.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike SQuery old_hlife.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery pkill.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery q2a.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery q3a.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery devi.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery qworld.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery rene.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike SQuery rvbshld.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery savage.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery simracer.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery sof1.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery sof2.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery unreal.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery ut2004.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike SQuery vietcong.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery doom3.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery armygame.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1610  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery et.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery flashpoint.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery gameSpy.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery gameSpy2.php libpath Parameter PHP File Include	CWE: 94  CVE: 2006-1688  BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.

Name	References	Description
Strike SQuery gore.php libpath Parameter PHP File Include	CWE: 94 CVE: 2006-1688 BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike SQuery gsvari.php libpath Parameter PHP File Include	CWE: 94 CVE: 2006-1688 BID: 17434	This strike exploits a PHP include flaw in the SQuery web application.
Strike Squid HTTP header buffer overflow	CWE: 119 CVE: 2013-4115 BID: 61111	This strike exploits a buffer overflow vulnerability in Squid. This vulnerability is due to improper handle large header in HTTP request.
Strike Sun Java System Web Server 7.0u7 Digest Auth Heap Overflow		This strike exploits a heap overflow in the Auth Digest field of the Sun Java web server.
Strike Sun Java Web Start dnsResolve ActiveX Buffer Overflow	CWE: 119 CVE: 2007-5019 BID: 25734	This strike exploits a buffer overflow vulnerability present in the isInstalled.dnsResolve ActiveX method installed with Sun Java's Web Start.
Strike NetWin SurgeMail Webmail Server page Parameter Format String	CWE: 134 CVE: 2008-1055 BID: 27990	This strike simulates a format string attack against the NetWin SurgeMail webmail server.
Strike ThemeREX Addons WordPress Plugin Remote Code Execution		A remote code execution vulnerability exists in ThemeREX Addons WordPress Plugin versions greater than 1.6.50, due to lack of sanitization for user-supplied data. By sending a crafted REST-API request to '/wp-json/trx_addons/v2/get/sc_layout', a remote unauthenticated user may invoke arbitrary PHP functions via 'sc' parameter.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike TheWebForum login.php username Parameter SQL Injection	CVE: 2006-0135 BID: 16161	This strike exploits a SQL injection flaw in the TheWebForum web application.
Strike TheWebForum register.php www Parameter XSS	CVE: 2006-0134 BID: 16161	This strike exploits a cross site scripting flaw in the TheWebForum web application.
Strike ThinkPHP Remote Code Execution	EXPLOITDB : 45978	This strike exploits a remote code execution in ThinkPHP framework. The flaw is rooted within the 'invokefunction' method as a consequence of no parameter validation. A remote, unauthenticated attacker may thus be able to execute code on the vulnerable machine with the permissions of the user running the web server.
Strike Microsoft IIS DLL Tilde Request Variant 1	CWE: 20 CVE: 2005-4360 BID: 15921	This strike attempts to crash IIS 5.1 by sending a malformed request.
Strike Microsoft IIS DLL Tilde Request Variant 2	CWE: 20 CVE: 2005-4360 BID: 15921	This strike attempts to crash IIS 5.1 by sending a malformed request.
Strike Microsoft IIS DLL Tilde Request Variant 3	CWE: 20 CVE: 2005-4360 BID: 15921	This strike attempts to crash IIS 5.1 by sending a malformed request.
Strike Microsoft IIS DLL Tilde Request Variant 4	CWE: 20 CVE: 2005-4360 BID: 15921	This strike attempts to crash IIS 5.1 by sending a malformed request.
Strike TinyPHPForum action.php txt Parameter XSS	CVE: 2006-0102	This strike exploits a cross site scripting flaw in the TinyPHPForum web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Trend Micro ObjectRemoveCtrl Server Method ActiveX	BID: 30407 CWE: 119 CVE: 2008-3364	This strike simulates an attack against Trend Micro OfficeScan. OfficeScanRemoveCtrl.dll is vulnerable to memory corruption when setting the Server attribute.
Strike TSEP colorsswitch.php tsep_config[absPath] Parameter PHP File Include	CVE: 2006-4055 BID: 19326	This strike exploits a PHP remote file include flaw in The Search Engine Project TSEP web application.
Strike Tumbleweed SecureTransport FileTransfer ActiveX Stack Overflow	CWE: 119 CVE: 2008-1724 BID: 28662	This strike exploits a flaw in the Tumbleweed SecureTransport FileTransfer ActiveX caused by improper checks on the "remoteFile" parameter of the "TransferFile" method.
Strike Ultimate Fun Book function.php gbpfad Parameter PHP File Include	CVE: 2007-1059 BID: 22633	This strike exploits a PHP include flaw in the Ultimate Fun Book web application.
Strike Ultimate PHP Board User-Agent HTTP Header Code Execution	CVE: 2003-0395	This strike exploits a code execution flaw in the Ultimate PHP Board web application.
Strike Ultra Crypto Component (CryptoX.dll) AcquireContext() Buffer Overflow	BID: 25609 CWE: 119 CVE: 2007-4903	This strike exploits a buffer overflow in the Ultra Crypto Component
Strike Ultra Crypto Component (CryptoX.dll) Insecure Method	BID: 25611 CWE: 22 CVE: 2007-4902	This strike exploits a flaw in CryptoX.dll that allows a webpage to save arbitrary data to any location on a disk.
Strike uTorrent announce Buffer Overflow (HTTP)	BID: 22530 CVE: 2007-0927	This strike exploits a buffer overflow in uTorrent caused by a torrent file with an 'announce' url that is too long

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike vCard 2.6 create.php uploaded Cross-Site Scripting	CWE: 79  CVE: 2006-1230  BID: 22819	This strike exploits a cross-site scripting vulnerability in vCard 2.6
Strike VEGO Web Forum index.php theme_id Parameter SQL Injection Variant 1	CVE: 2006-0065  BID: 16107	This strike exploits a SQL injection flaw in the VEGO web forum.
Strike VEGO Web Forum Pre-v1.26 index.php theme_id Parameter SQL Injection	CVE: 2006-0065  BID: 16107	This strike exploits a SQL injection flaw in the VEGO web forum.
Strike VEGO Web Forum index.php theme_id Parameter SQL Injection Variant 2	CVE: 2006-0065  BID: 16107	This strike exploits a SQL injection flaw in the VEGO web forum.
Strike VEGO Web Forum index.php theme_id Parameter SQL Injection Variant 2 (<v1.26)	CVE: 2006-0065  BID: 16107	This strike exploits a SQL injection flaw in the VEGO web forum.
Strike VEGO Web Forum login.php username Parameter SQL Injection	CVE: 2006-0067  BID: 16108	This strike exploits a SQL injection flaw in the VEGO web forum.
Strike Venom Board post.php3 topic_id Parameter SQL Injection	CWE: 89  CVE: 2006-0160  BID: 16176	This strike exploits a SQL injection flaw in the Venom Board web application.
Strike VLC HTTPD Connection Header Format String	CVE: 2007-6682  BID: 27015	This strike exploits a format string vulnerability in the HTTPD interface of the VLC media player.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike VLC Ogg Vorbis Comment Header Format String (HTTP)	BID: 24555  CVE: 2007-3316	This strike exploits a format string vulnerability in VLC when decoding Ogg Vorbis files. This strike simulates downloading a malicious file via HTTP.
Strike VLC udp -- Handler Format String Variant 1	CWE: 134  CVE: 2007-0017  BID: 21852	This strike exploits a format string vulnerability in the VLC video player. This exploit simulates a download of the exploit over HTTP on port 80. This version of the exploit targets the i386 processor architecture.
Strike VLC udp -- Handler Format String Variant 2	CWE: 134  CVE: 2007-0017  BID: 21852	This strike exploits a format string vulnerability in the VLC video player. This exploit simulates a download of the exploit over HTTP on port 80. This version of the exploit targets the PPC processor architecture.
Strike VideoLan Player XSPF Identifier Memory Corruption	CWE: 399  CVE: 2008-4558  BID: 31758	This strike triggers a vulnerability in the VideoLan player when handling XSPF files with a crafted identifier attribute.
Strike Vmist Downstat chart.php art Parameter PHP File Include	CVE: 2006-4827  BID: 20007	This strike exploits a PHP include flaw in the Vmist Downstat web application.
Strike Vmist Downstat admin.php art Parameter PHP File Include	CVE: 2006-4827  BID: 20007	This strike exploits a PHP include flaw in the Vmist Downstat web application.
Strike Vmist Downstat modes.php art Parameter PHP File Include	CVE: 2006-4827  BID: 20007	This strike exploits a PHP include flaw in the Vmist Downstat web application.
Strike Vmist Downstat stats.php art Parameter PHP File Include	CVE: 2006-4827  BID: 20007	This strike exploits a PHP include flaw in the Vmist Downstat web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike VMware Workstation ActiveX Control (vielib.dll) Remote Code Execution	CVE: 2007-4155 BID: 25131	Absolute path traversal vulnerability in a certain ActiveX control in vielib.dll in EMC VMware 6.0.0 allows remote attackers to execute arbitrary local programs via a full pathname in the first two arguments to the (1) CreateProcess or (2) CreateProcessEx method. This strike delivers a payload consistent with abusing parameters within the context of the former method, namely CreateProcess() and targets a Windows machine (any version) running Internet Explorer (any version) and attempts to run binaries found on a stock Windows XP SP3 x86 install (some binaries included in this strike's potential payloads may not be included in every Windows release).
Strike Voodoo Chat index.php file path Parameter PHP File Include	CVE: 2006-3991 BID: 19277	This strike exploits a PHP include flaw in the Voodoo Chat web application.
Strike VS News System show_news_inc.php newsordner Parameter PHP File Include	CVE: 2007-1017 BID: 22592	This strike exploits a PHP include flaw in VS News System.
Strike WebBBS webbbs_config.pl followup Parameter Shell Execution	CVE: 2002-1993 BID: 5048	This strike exploits a remote command execution flaw in the WebBBS bulletin board application.
Strike Microsoft IIS WebHits Authentication Bypass	CWE: 264 CVE: 2007-2815 BID: 24105	This strike simulates an attacker exploiting the authentication bypass flaw exposed by the WebHits ISAPI filter.
Strike Nullsoft Winamp AIFF File Format Header Parsing Memory Corruption	CWE: 119 CVE: 2009-0263 BID: 33226	This strike sends a malicious AIFF file that causes a head overflow in Winamp when it is parsed.
Strike Nullsoft Winamp PLS File Handling Buffer Overflow	CVE: 2006-0476 BID: 16410	This strike exploits a flaw in Winamp's handling of PLS files containing a long file name entry.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Windows Explorer.exe AVI Right Click Denial of Service (HTTP)	CVE: 2007-0562	This strike exploits a denial of service condition in Microsoft Windows explorer.exe when right-clicking on a malformed AVI file.
Strike Microsoft Windows Contact File HTML injection	EXPLOITDB : 46222	This strike executes a vulnerability in a Microsoft Windows Contact file. Specifically a remote attacker can execute arbitrary code on Microsoft Windows by performing code injection in the email field of a Windows Contact file.
Strike Windows Help Center Malformed Escape Sequence Command Execution	CWE: 78 CVE: 2010-1885 BID: 40725	This strike exploits a vulnerability present in Microsoft's Windows Help Center protocol in which a malformed escape character sequence will bypass allowlist protections and allow an attacker to run arbitrary commands in the context of the user.
Strike Alt-N WebAdmin USER Buffer Overflow	BID: 8024 CVE: 2003-0471	This strike exploits a buffer overflow in the Alt-N WebAdmin service (webAdmin.dll version: 2.0.4) and causes arbitrary code execution conditions.
Strike Windows SMB Redirect		This strike exploits an information disclosure vulnerability in Microsoft Windows. The vulnerability is due to the use of Windows API functions that automatically attempt to authenticate with an SMB server pointed to by a file:// url. By intercepting an HTTP request and responding with an HTTP Redirect pointing to a malicious SMB server, an attacker could get access to encrypted user credentials, for offline decryption.
Strike Microsoft Windows Color Management Module ICC Profile Buffer Overflow (HTTP)	CVE: 2005-1219 BID: 14214	Microsoft Windows has a buffer overflow vulnerability in the processing of malformed image files. This strike simulates downloading a JPEG via HTTP.
Strike Windows OLE32.dll Word Document Handling Denial of Service (HTTP)	CWE: 119 CVE: 2007-1347 BID: 22847	This strike exploits a denial of service condition in Microsoft Windows OLE32.dll when parsing a malicious Word document.
Strike Microsoft Windows Remote Desktop Web Access XSS	CWE: 79 CVE: 2011-1263	This strike triggers a cross-site scripting vulnerability in the Microsoft Windows Remote Desktop Web Access service.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Wing FTP Server Lua Console Remote Code Execution	EXPLOITDB : 48676	A remote code execution vulnerability exists in Wing FTP Server due to lack of user input sanitization for the Lua Console feature. By sending a crafted 'command' POST parameter, an authenticated user could execute arbitrary commands as the superuser.
Strike Winzip ActiveX CreateNewFolderFromName Buffer Overflow	CWE: 119 CVE: 2006-6884	This strike exploits a buffer overflow in the CreateNewFolderFromName function in the WZFILEVIEW.FileViewCtrl.61 ActiveX control.
Strike Wireshark packet-dect.c Stack Buffer Overflow (HTTP)	CWE: 119 CVE: 2011-1591	This strike exploits a stack buffer overflow vulnerability present in Wireshark <= 1.4.4 by crafting a malicious PCAP file. When this flaw is triggered successfully, remote code execution is possible allowing for arbitrary code to run in the context of user running Wireshark.
Strike Wireshark Profinet DCP Dissector Name of Station Set Request Format String Vulnerability		This strike triggers a denial of service vulnerability in the Wireshark network protocol analyzer. The method for triggering the vulnerability is to transfer a malicious pcap file over the HTTP protocol.
Strike Wireshark Profinet DCP Dissector Ident Reponse Format String Vulnerability		This strike triggers a denial of service vulnerability in the Wireshark network protocol analyzer. The method for triggering the vulnerability is to transfer a malicious pcap file over the HTTP protocol.
Strike Windows Metafile (WMF) SetAbortProc() Code Execution [001]	BID: 16074 CWE: 20 CVE: 2005-4560	This strike exploits a vulnerability in the GDI library included with Windows XP, 2003, and Vista. This vulnerability uses the 'Escape' metafile function to execute arbitrary code through the SetAbortProc procedure.
Strike Windows Metafile (WMF) SetAbortProc() Code Execution [002]	BID: 16074 CWE: 20 CVE: 2005-4560	This strike exploits a vulnerability in the GDI library included with Windows XP, 2003, and Vista. This vulnerability uses the 'Escape' metafile function to execute arbitrary code through the SetAbortProc procedure.
Strike Windows Metafile (WMF) SetAbortProc() Code Execution [003]	BID: 16074 CWE: 20 CVE: 2005-4560	This strike exploits a vulnerability in the GDI library included with Windows XP, 2003, and Vista. This vulnerability uses the 'Escape' metafile function to execute arbitrary code through the SetAbortProc procedure.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Windows Metafile (WMF) SetAbortProc() Code Execution [004]	BID: 16074  CWE: 20  CVE: 2005-4560	This strike exploits a vulnerability in the GDI library included with Windows XP, 2003, and Vista. This vulnerability uses the 'Escape' metafile function to execute arbitrary code through the SetAbortProc procedure.
Strike Windows Metafile (WMF) SetAbortProc() Code Execution [005]	BID: 16074  CWE: 20  CVE: 2005-4560	This strike exploits a vulnerability in the GDI library included with Windows XP, 2003, and Vista. This vulnerability uses the 'Escape' metafile function to execute arbitrary code through the SetAbortProc procedure.
Strike Windows Metafile (WMF) SetAbortProc() Code Execution [006]	BID: 16074  CWE: 20  CVE: 2005-4560	This strike exploits a vulnerability in the GDI library included with Windows XP, 2003, and Vista. This vulnerability uses the 'Escape' metafile function to execute arbitrary code through the SetAbortProc procedure.
Strike Windows Metafile (WMF) SetAbortProc() Code Execution [007]	BID: 16074  CWE: 20  CVE: 2005-4560	This strike exploits a vulnerability in the GDI library included with Windows XP, 2003, and Vista. This vulnerability uses the 'Escape' metafile function to execute arbitrary code through the SetAbortProc procedure.
Strike Windows Metafile (WMF) SetAbortProc() Code Execution [008]	BID: 16074  CWE: 20  CVE: 2005-4560	This strike exploits a vulnerability in the GDI library included with Windows XP, 2003, and Vista. This vulnerability uses the 'Escape' metafile function to execute arbitrary code through the SetAbortProc procedure.
Strike Windows Metafile (WMF) SetAbortProc() Code Execution [009]	BID: 16074  CWE: 20  CVE: 2005-4560	This strike exploits a vulnerability in the GDI library included with Windows XP, 2003, and Vista. This vulnerability uses the 'Escape' metafile function to execute arbitrary code through the SetAbortProc procedure.
Strike Windows Metafile (WMF) SetAbortProc() Code Execution [010]	BID: 16074  CWE: 20  CVE: 2005-4560	This strike exploits a vulnerability in the GDI library included with Windows XP, 2003, and Vista. This vulnerability uses the 'Escape' metafile function to execute arbitrary code through the SetAbortProc procedure.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Windows Metafile (WMF) SetAbortProc() Code Execution [011]	BID: 16074 CWE: 20 CVE: 2005-4560	This strike exploits a vulnerability in the GDI library included with Windows XP, 2003, and Vista. This vulnerability uses the 'Escape' metafile function to execute arbitrary code through the SetAbortProc procedure.
Strike Windows Metafile (WMF) SetAbortProc() Code Execution [012]	BID: 16074 CWE: 20 CVE: 2005-4560	This strike exploits a vulnerability in the GDI library included with Windows XP, 2003, and Vista. This vulnerability uses the 'Escape' metafile function to execute arbitrary code through the SetAbortProc procedure.
Strike Windows Metafile (WMF) SetAbortProc() Code Execution [013]	BID: 16074 CWE: 20 CVE: 2005-4560	This strike exploits a vulnerability in the GDI library included with Windows XP, 2003, and Vista. This vulnerability uses the 'Escape' metafile function to execute arbitrary code through the SetAbortProc procedure.
Strike WMITools WBEMSingleView.ocx ActiveX Remote Command Execution	CWE: 94 CVE: 2010-3973 BID: 45546	The WBEMSingleView.ocx ActiveX control that is included with WMITools contains at least two methods that allow a user to directly reference a given memory address and can lead to remote code execution.
Strike WMNews index.php base_datapath Parameter PHP File Include	CVE: 2006-3928 BID: 19187	This strike exploits a PHP include flaw in the WMNews web application.
Strike Word Macro HTTP Exfiltration Macro-enabled VBA Maldoc Command and control		This strikes exfiltrates host information via HTTP POST request.
Strike Wordcircle index.php password Parameter SQL Injection	CWE: 89 CVE: 2006-0205 BID: 16227	This strike exploits a SQL injection flaw in the Wordcircle web application.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft WordPad Embedded COM Code Execution (InstallEngine) (HTTP)		This strike exploits a flaw in Microsoft WordPad that can be used to execute arbitrary code. This particular strike embeds the InstallEngine COM control into the OLE section of a WordPad RTF document.
Strike Microsoft WordPad Embedded COM Code Execution (Sysmon.3) (HTTP)		This strike exploits a flaw in Microsoft WordPad that can be used to execute arbitrary code. This particular strike embeds the Sysmon.3 COM control into the OLE section of a WordPad RTF document and defines a set of corrupt OLE properties that will cause a crash on load.
Strike WordPress Plugin WP with Spritz 1.0 Remote File Inclusion	EXPLOITDB : 44544	This strike exploits a remote file inclusion vulnerability in WordPress Plugin WP Spritz 1.0. The vulnerability is due to improper sanitization of the "url" parameter. By successfully exploiting this vulnerability, a remote, unauthenticated attacker could retrieve arbitrary files from the target server.
Strike Wordpress Download Manager Plugin Remote File Upload		A remote file upload vulnerability exists in Wordpress Download Manager Plugin versions prior to 2.7.5. This vulnerability allows an unauthenticated attacker to upload a file to the web server and could facilitate remote code execution with the privileges of the account running the web server application.
Strike WordPress Backdoor ix Parameter Eval	CWE: 20 CVE: 2007-1277 BID: 22797	The source code to WordPress was backdoored in February 2007 to pass the ix parameter to the php eval() function.
Strike WordPress Backdoor iz Parameter Passthru	CWE: 20 CVE: 2007-1277 BID: 22797	The source code to WordPress was backdoored in February 2007 to pass the iz parameter to the php passthru() function.
Strike Wordpress Mobile Detector Plugin Remote File Upload		This strike exploits an unauthenticated file-upload vulnerability in WordPress Mobile-Detector plugin. The vulnerability is due to insufficient validation of user input A remote file upload vulnerability exists in Wordpress Download Manager Plugin versions prior to 2.7.5. This vulnerability allows an unauthenticated attacker to upload a file to the web server and could facilitate remote code execution with the privileges of the account running the web server application.
Strike Wordpress page-flip-image-gallery plugins Remote File Upload		This strike exploits a remote file upload vulnerability inside wordpress page flip image gallery plugin.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike WordPress MapSVG Lite Plugin Stored Cross-Site Scripting		This strike exploits a stored Cross-Site Scripting vulnerability in WordPress MapSVG Plugin. The vulnerability is a consequence of no user input sanitization when storing the 'data[mapsvg_data]'. A successful exploitation leads to arbitrary code execution in visitors' browsers or credentials theft.
Strike WordPress Property Plugin PHP File Upload Code Execution	BID: 53787	This strike identifies a vulnerability in the WordPress Property plugin. Due to improper validation, a user can upload a file to a temporary directory that will allow for remote code to be executed.
Strike WoW Roster conf.php subdir Parameter PHP File Include	CVE: 2006-3997 CVE: 2006-3998 BID: 19269	This strike exploits a PHP include flaw in WoW Roster web application.
Strike WoW Roster hsList.php subdir Parameter PHP File Include	CVE: 2006-3997 CVE: 2006-3998 BID: 19269	This strike exploits a PHP include flaw in WoW Roster web application.
Strike Netscape Server WP Tag Directory Index Variant 1	BID: 1063 CVE: 2000-0236	This strike attempts to obtain a directory listing from the web server by specifying a special request parameter.
Strike Netscape Server WP Tag Directory Index Variant 2	BID: 1063 CVE: 2000-0236	This strike attempts to obtain a directory listing from the web server by specifying a special request parameter.
Strike Netscape Server WP Tag Directory Index Variant 3	BID: 1063 CVE: 2000-0236	This strike attempts to obtain a directory listing from the web server by specifying a special request parameter.
Strike Netscape Server WP Tag Directory Index Variant 4	BID: 1063 CVE: 2000-0236	This strike attempts to obtain a directory listing from the web server by specifying a special request parameter.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Netscape Server WP Tag Directory Index Variant 6	BID: 1063 CVE: 2000-0236	This strike attempts to obtain a directory listing from the web server by specifying a special request parameter.
Strike Netscape Server WP Tag Directory Index Variant 7	BID: 1063 CVE: 2000-0236	This strike attempts to obtain a directory listing from the web server by specifying a special request parameter.
Strike Netscape Server WP Tag Directory Index Variant 8	BID: 1063 CVE: 2000-0236	This strike attempts to obtain a directory listing from the web server by specifying a special request parameter.
Strike Netscape Server WP Tag Directory Index Variant 9	BID: 1063 CVE: 2000-0236	This strike attempts to obtain a directory listing from the web server by specifying a special request parameter.
Strike X97EmbedAn Excel Document (http)	BID: 18422 CVE: 2006-3059	The X97EmbedAn malware abuses an arbitrary code execution flaw in Microsoft Office.
Strike Joomla Plugin Mod_simplefileupload File Upload		This strike exploits a file upload vulnerability present in Joomla mod_simplefileupload plugin. By exploiting this vulnerability, an unauthenticated attacker can run arbitrary code by uploading files on the server and execute them. Note: This vulnerability was disclosed by the XAttacker tool.
Strike XAttacker Tool Prestashop Addons Arbitrary File Upload		This strike exploits file upload vulnerabilities in Prestashop CMS addons targeted by recently published XAttacker Tool. The main issue is the lack of sanitization of the user-supplied files by the components in charge of handling files upload queries. By exploiting these vulnerabilities, an unauthenticated attacker can run arbitrary code by uploading files on the server and execute them.
Strike XAttacker Tool WordPress Plugins Arbitrary File Upload (verified)	CVE: 2015-2825 EXPLOITDB : 36374 EXPLOITDB : 34922 EXPLOITDB : 36640	This strike exploits a series of file upload vulnerabilities in different Wordpress Plugins targeted by recently published XAttacker Tool. The common issue is the lack of sanitization of the user-uploaded files in the components in charge of handling files upload queries. By exploiting this vulnerabilities, an unauthenticated attacker can run arbitrary code by uploading files on the server and execute them.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Xitami Web Server If-Modified-Since Buffer Overflow	CWE: 119 CVE: 2007-5067 BID: 25772	This strike exploits a buffer overflow in the Xitami web server when handling a long If-Modified-Since HTTP header.
Strike Yahoo Toolbar ActiveX Control Denial of Service	BID: 26656 CWE: 119 CVE: 2007-6228	This strike causes a denial of service in the Yahoo Toolbar browser plugin's ActiveX control.
Strike SQL Injection Vulnerability In ManageEngine OpManager		This strike exploits an SQL injection vulnerability in ManageEngine OpManager. The vulnerability is due to improper validation of agentKey HTTP parameter. An attacker could exploit this vulnerability by sending an unauthenticated malicious request to the server, compromising the integrity of the database.
Strike Multiple ManageEngine Products It360SPUtil SQL Injection		This strike exploits an SQL injection vulnerability in ManageEngine Applications Manager and ManageEngine IT360 MSP Edition. The vulnerability is due to improper validation of It360SPUtil resIds HTTP parameter. An attacker could exploit this vulnerability by sending an unauthenticated malicious request to the server, compromising the integrity of the database.
Strike ManageEngine Applications Manager CommonAPIUtil SQL Injection		This strike exploits an SQL injection vulnerability in ManageEngine Applications Manager. The vulnerability is due to improper validation of groupId HTTP parameter. An attacker could exploit this vulnerability by sending an unauthenticated malicious requests to the server, compromising the integrity of the database.
Strike AuthenticationFilter Policy Bypass Vulnerability Inside SolarWinds Storage Manager	CVE: 2015-5371	This strike exploits a policy bypass vulnerability inside SolarWinds Storage Manager. The vulnerability is due to lack of authenticating HTTP requests to certain URIs. An attacker could exploit this vulnerability in order to upload malicious scripts and then remotely execute them.
Strike Borland AccuRev savecontent fname Directory Traversal		This strike exploits a directory traversal vulnerability in Borland AccuRev. The fname parameter in HTTP requests to /accurev/webgui/savecontent is not sanitized for directory traversal characters. An attacker may set an fname ending in ".csv" or ".xml" to read any arbitrary csv or xml file, or may request any other file on the system in order to delete the file. Successful exploitation may result in disclosure of arbitrary csv or xml files or deletion of arbitrary files on the system, which may result in a denial of service condition.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Reprise License Manager actserver akey Buffer Overflow Vulnerability	CWE: 119 CVE: 2015-6946	This strike exploits a buffer overflow vulnerability in Reprise License Manager. The vulnerability is due to improper validation of HTTP actserver and akey parameters. An attacker could exploit this vulnerability in order to remotely execute code on the target machine.
Strike Reprise License Manager Directory Traversal Vulnerability Through outputfile Parameter		This strike exploits a directory traversal vulnerability in Reprise License Manager. The vulnerability is due to improper validation of HTTP outputfile parameter. An attacker could exploit this vulnerability in order to gain unauthorized access to information or services.
Strike Reprise License Manager Directory Traversal Vulnerability Through lf parameter		This strike exploits a directory traversal vulnerability in Reprise License Manager. The vulnerability is due to improper validation of HTTP lf parameter. An attacker could exploit this vulnerability in order to gain unauthorized access to information or services.
Strike Reprise License Manager Directory Traversal Vulnerability Through lf parameter		This strike exploits a directory traversal vulnerability in Reprise License Manager. The vulnerability is due to improper validation of HTTP lf parameter in requests to /goform/edit_lf_process URI. An attacker could exploit this vulnerability in order to gain unauthorized access to information or services.
Strike Trend Micro Safe Sync Reconnect Query String Multiple Parameters Command Injection		This strike exploits a command execution vulnerability in Trend Micro Safe Sync. Several query string parameters accepted by the reconnect command are vulnerable to command injection. An authenticated attacker can connect, disconnect, and then send a specially crafted HTTP command to reconnect in order to achieve arbitrary code execution with root privileges.
Strike Trend Micro IWSVA deploywizard haport Parameter Command Injection		This strike exploits a command execution vulnerability in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The haport parameter, which is sent in HTTP GET requests to the /deploywizard/deploywizard.do uri, is vulnerable to command injection and is not sanitized. An attacker can send a specially crafted HTTP GET request to achieve arbitrary command execution. NOTE: By default the vulnerable services are accessed via SSL connection (port 8443)
Strike Trend Micro IWSVA Domain List bdn Parameter Command Injection		This strike exploits a command execution vulnerability in Trend Micro InterScan Web Security Virtual Appliance (IWSVA). The bdn parameter, which is sent in HTTP POST requests to the /rest/domains uri, is vulnerable to command injection and is not sanitized. An attacker can send a specially crafted HTTP POST request to achieve arbitrary command execution. NOTE: By default the vulnerable services are accessed via SSL connection (port 8443)
Strike ZebraFeeds controller.php zf_path Parameter PHP File Include	CVE: 2007-1010 BID: 22576	This strike exploits a PHP include flaw in ZebraFeeds 1.1.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Novell ZENworks Configuration Management UploadServlet File Upload and Code Execution	CWE: 22 CVE: 2010-5324 BID: 39114	This strike exploits a file upload vulnerability that exists in the ZENworks Configuration Management server. If a user uses directory traversal characters, they can access the Upload Servlet application, upload a file then make another request to execute it.
Strike Microsoft SharePoint WSDL DISCO Inifinate Loop Denial of Service	CWE: 20 CVE: 2013-0081 BID: 62205	Microsoft SharePoint contains a denial of service vulnerability. When a non-existent custom web application is requested, the program will enter an infinite loop while searching for the web application, resulting in a denial of service condition.
Strike Arcserve Unified Data Protection Console Multiple Directory Traversal Vulnerabilities	CWE: 22 CVE: 2015-4068 BID: 74845	This strike exploits a directory traversal vulnerability in Arcserve Unified Data Protection prior to version 5.0 update 4. The vulnerability is caused by improper validation of a file path supplied by the user in the export and reportFile servlets. A remote, unauthenticated attacker could exploit this by sending crafted requests to the application, leading to denial-of-service, information disclosure and, possibly, loss of information.
Strike Oracle WebLogic Server Directory Traversal Vulnerability	CVE: 2020-14750 CWE: 22	This strike exploits a directory traversal vulnerability in Oracle WebLogic Server. The vulnerability arises due to improper input validation which allows attackers to bypass authentication mechanisms. A remote, unauthenticated attacker can send crafted HTTP requests containing double encoded directory traversal sequences to access restricted paths such as console.portal without proper authentication. Successful exploitation could lead to remote code execution, potentially resulting in full compromise of the Oracle WebLogic Server.
Strike Sun Java Plugin JNLP Argument Injection (Debug)	BID: 12847 CVE: 2005-0418 CVE: 2005-0836	This strike exploits a flaw in the Sun Java plugin that allows arbitrary code execution through malicious JNLP files.
Strike Sun Java Plugin JNLP Argument Injection (Policy)	BID: 12847 CVE: 2005-0418 CVE: 2005-0836	This strike exploits a flaw in the Sun Java plugin that allows arbitrary code execution through malicious JNLP files.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Apple OS X QuickDraw GetSrcBits32ARGB Memory Corruption Denial of Service (IMAP4)	BID: 22207  CVE: 2007-0462	This strike exploits a denial of service condition in Apple's Mac OS X when opening a malformed PICT file.
Strike Microsoft Excel NULL Pointer DoS (A) (IMAP4)	BID: 22717  CVE: 2007-1239	This strike exploits a denial of service flaw in Microsoft Excel using a corrupted XLS document.
Strike Microsoft Excel NULL Pointer DoS (B) (IMAP4)	BID: 22717  CVE: 2007-1239	This strike exploits a denial of service flaw in Microsoft Excel using a corrupted XLS document.
Strike Chicken of the VNC Hostname Size Denial of Service	CVE: 2007-0756  BID: 22372	This strike causes a denial of service in the Chicken of the VNC client program by specifying a long hostname length field in a VNC server.
Strike Adobe Acrobat Reader getIcon Memory Corruption (IMAP4 Base64)	BID: 34169  CWE: 20  CVE: 2009-0927	This strike exploits a flaw in Adobe's PDF reader that can result in the execution of arbitrary code.
Strike Adobe Acrobat Reader getIcon Memory Corruption (IMAP4 Quoted Printable)	BID: 34169  CWE: 20  CVE: 2009-0927	This strike exploits a flaw in Adobe's PDF reader that can result in the execution of arbitrary code.
Strike GDI+ PNG Integer Overflow Vulnerability (IMAP4 Quoted Printable)	CWE: 189  CVE: 2009-3126	This strike exploits the way the buffer size for the pixel data in interlaced PNGs is calculated by GDI+. The methods used by GDI+ contain integer overflow vulnerabilities.
Strike Windows Media Player ASX File Heap Overflow (IMAP4 Base64)	CWE: 119  CVE: 2006-6134  BID: 21247	Microsoft Windows Media Player contains a vulnerability that will cause memory corruption when a malicious *.asx file is opened

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Windows Media Player ASX File Heap Overflow (IMAP4 Quoted Printable)	CWE: 119 CVE: 2006-6134 BID: 21247	Microsoft Windows Media Player contains a vulnerability that will cause memory corruption when a malicious *.asx file is opened
Strike Microsoft Windows AVIFile Media File Truncation Code Execution (IMAP4 Base64)	BID: 35967 CWE: 94 CVE: 2009-1545	This strike exploits a vulnerability in Microsoft Windows when parsing an AVI file with truncated AVIH chunk data.
Strike Digium Asterisk Manager Shell Execution	CWE: 287 CVE: 2012-2414 BID: 53206	This strike exposes an ability for an authenticated user to run an arbitrary shell command without restriction.
Strike Internet Explorer EMF File Rendering Denial of Service (IMAP4)	CWE: 399 CVE: 2005-0803 BID: 12834	This strike exploits a denial of service flaw in Microsoft Windows. This flaw is triggered through a malformed Windows EMF Metafile. This strike simulates downloading an EMF file via IMAP4.
Strike Microsoft Windows LoadImage API Overflow (IMAP4)	BID: 12095 CVE: 2004-1049	This strike exploits a flaw in the parsing of images via LoadImage on Microsoft Windows. This strike simulates downloading a malicious .ani animated cursor in an IMAP4 message.
Strike MWindows Mail HTML Link Program Execution (IMAP4)	BID: 23103 CVE: 2007-1658	This strike exploits an arbitrary program execution flaw in the Windows Mail client. This flaw is triggered when a user clicks a hyperlink within an HTML email.
Strike MWindows Mail HTML Link Program Execution UNC (IMAP4)	BID: 23103 CVE: 2007-1658	This strike exploits an arbitrary program execution flaw in the Windows Mail client. This flaw is triggered when a user clicks a hyperlink within an HTML email.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Windows Vista Contact Gadget Remote Code Execution (IMAP4)	CVE: 2007-3032 BID: 25304	This strike exploits a flaw in the Contact Gadget in Microsoft Vista when displaying a malicious contact.
Strike Microsoft Word RTF Object Parsing Vulnerability (dpendgroup) (IMAP4 Base64)	CWE: 399 CVE: 2008-4030	This strike exploits a vulnerability in MS Word caused by an RTF file with invalid '\dpendgroup' directives.
Strike UNIX rlogind Service -root Authentication Bypass	CVE: 1999-0113 BID: 458	This strike exploits an authentication bypass vulnerability present in certain versions of the rlogin service.
Strike Microsoft Windows SMB NT Rename Buffer Overflow	CWE: 20 CVE: 2017-0146 BID: 96707	This strike exploits a buffer overflow vulnerability in Microsoft Windows SMB Service. The vulnerability can be triggered by sending an overly large NT Trans request. A remote, unauthenticated attacker could exploit this vulnerability to execute arbitrary code on the target system. * NOTE: This vulnerability was targeted with ShadowBrokers EternalChampion exploit
Strike Microsoft Windows SMB Information Disclosure	CWE: 200 CVE: 2017-0147 BID: 96709	This strike exploits an information disclosure vulnerability in Microsoft Windows SMB Service. The vulnerability can be triggered by sending an SMB request that reads beyond a boundary. A remote, unauthenticated attacker could exploit this vulnerability to reveal memory addresses for use with other exploits. * NOTE: This vulnerability was targeted with ShadowBrokers EternalChampion exploit
Strike SSLv2 DROWN decryption	CWE: 200 CVE: 2016-0800 CVE: 2016-0703	This strike simulates traffic which may be seen during the man-in-the-middle DROWN SSLv2 decryption attack. In order to gather enough data to break encryption, an attacker may initiate several thousand SSLv2 handshakes. This strike initiates only 100 handshakes to reduce test time, however, because the recommended remediation is to completely disable SSLv2, even one handshake should be viewed as suspicious.
Strike Cisco NX-OS Command Injection	BID: 50347 CWE: 264 CVE: 2011-2569	This strike exploits a vulnerability in the input sanitization of Cisco's NX-OS which allows for command injection when output is piped to certain commands (less, section). This can be used to achieve privilege escalation.

Name	References	Description
Strike Oracle WebLogic Server Insecure Deserialization - RCE	CWE: 502 CVE: 2018-2628 BID: 103776	An insecure deserialization vulnerability was found in Oracle WebLogic Server due to insufficient validation of serialized data. Vulnerability can be exploited by sending a specially crafted serialized object. Successful exploitation can result in arbitrary code execution in the context of the user running WebLogic.
Strike Magento API unserialize Remote Code Execution	CWE: 74 CVE: 2016-4010	Magento CE and EE before 2.0.6 allows remote attackers to conduct PHP objection injection attacks and execute arbitrary PHP code via crafted serialized shopping cart data.
Strike AI LLM Prompt Injection ASCII Art Font Alphabet - Gemini		This strike sends an ASCII Art-based Jailbreak Prompt of font Alphabet to the Gemini LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Gemini LLM. Target LLM: Gemini
Strike AI LLM Prompt Injection ASCII Art Font Alphabet - Grok		This strike sends an ASCII Art-based Jailbreak Prompt of font Alphabet to the Grok LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Grok LLM. Target LLM: Grok
Strike AI LLM Prompt Injection ASCII Art Font Alphabet - OpenAI		This strike sends an ASCII Art-based Jailbreak Prompt of font Alphabet to the OpenAI LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the OpenAI LLM. Target LLM: OpenAI
Strike AI LLM Prompt Injection ASCII Art Font Binary - Gemini		This strike sends an ASCII Art-based Jailbreak Prompt of font Binary to the Gemini LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Gemini LLM. Target LLM: Gemini
Strike AI LLM Prompt Injection ASCII Art Font Binary - Grok		This strike sends an ASCII Art-based Jailbreak Prompt of font Binary to the Grok LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Grok LLM. Target LLM: Grok

Name	References	Description
Strike AI LLM Prompt Injection ASCII Art Font Binary - OpenAI		This strike sends an ASCII Art-based Jailbreak Prompt of font Binary to the OpenAI LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the OpenAI LLM. Target LLM: OpenAI
Strike AI LLM Prompt Injection ASCII Art Font Bubble - Gemini		This strike sends an ASCII Art-based Jailbreak Prompt of font Bubble to the Gemini LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Gemini LLM. Target LLM: Gemini
Strike AI LLM Prompt Injection ASCII Art Font Bubble - Grok		This strike sends an ASCII Art-based Jailbreak Prompt of font Bubble to the Grok LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Grok LLM. Target LLM: Grok
Strike AI LLM Prompt Injection ASCII Art Font Bubble - OpenAI		This strike sends an ASCII Art-based Jailbreak Prompt of font Bubble to the OpenAI LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the OpenAI LLM. Target LLM: OpenAI
Strike AI LLM Prompt Injection ASCII Art Font Digital - Gemini		This strike sends an ASCII Art-based Jailbreak Prompt of font Digital to the Gemini LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Gemini LLM. Target LLM: Gemini
Strike AI LLM Prompt Injection ASCII Art Font Digital - Grok		This strike sends an ASCII Art-based Jailbreak Prompt of font Digital to the Grok LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Grok LLM. Target LLM: Grok
Strike AI LLM Prompt Injection ASCII Art Font Digital - OpenAI		This strike sends an ASCII Art-based Jailbreak Prompt of font Digital to the OpenAI LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the OpenAI LLM. Target LLM: OpenAI
Strike AI LLM Prompt Injection ASCII Art Font Doh - Gemini		This strike sends an ASCII Art-based Jailbreak Prompt of font Doh to the Gemini LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Gemini LLM. Target LLM: Gemini

Name	References	Description
Strike AI LLM Prompt Injection ASCII Art Font Doh - Grok		This strike sends an ASCII Art-based Jailbreak Prompt of font Doh to the Grok LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Grok LLM. Target LLM: Grok
Strike AI LLM Prompt Injection ASCII Art Font Doh - OpenAI		This strike sends an ASCII Art-based Jailbreak Prompt of font Doh to the OpenAI LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the OpenAI LLM. Target LLM: OpenAI
Strike AI LLM Prompt Injection ASCII Art Font Dwhistled - Gemini		This strike sends an ASCII Art-based Jailbreak Prompt of font Dwhistled to the Gemini LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Gemini LLM. Target LLM: Gemini
Strike AI LLM Prompt Injection ASCII Art Font Dwhistled - Grok		This strike sends an ASCII Art-based Jailbreak Prompt of font Dwhistled to the Grok LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Grok LLM. Target LLM: Grok
Strike AI LLM Prompt Injection ASCII Art Font Dwhistled - OpenAI		This strike sends an ASCII Art-based Jailbreak Prompt of font Dwhistled to the OpenAI LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the OpenAI LLM. Target LLM: OpenAI
Strike AI LLM Prompt Injection ASCII Art Font Letters - Gemini		This strike sends an ASCII Art-based Jailbreak Prompt of font Letters to the Gemini LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Gemini LLM. Target LLM: Gemini
Strike AI LLM Prompt Injection ASCII Art Font Letters - Grok		This strike sends an ASCII Art-based Jailbreak Prompt of font Letters to the Grok LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Grok LLM. Target LLM: Grok
Strike AI LLM Prompt Injection ASCII Art Font Letters - OpenAI		This strike sends an ASCII Art-based Jailbreak Prompt of font Letters to the OpenAI LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the OpenAI LLM. Target LLM: OpenAI

Name	References	Description
Strike AI LLM Prompt Injection ASCII Art Font Mnemonic - Gemini		This strike sends an ASCII Art-based Jailbreak Prompt of font Mnemonic to the Gemini LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Gemini LLM. Target LLM: Gemini
Strike AI LLM Prompt Injection ASCII Art Font Mnemonic - Grok		This strike sends an ASCII Art-based Jailbreak Prompt of font Mnemonic to the Grok LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Grok LLM. Target LLM: Grok
Strike AI LLM Prompt Injection ASCII Art Font Mnemonic - OpenAI		This strike sends an ASCII Art-based Jailbreak Prompt of font Mnemonic to the OpenAI LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the OpenAI LLM. Target LLM: OpenAI
Strike AI LLM Prompt Injection ASCII Art Font Morse - Gemini		This strike sends an ASCII Art-based Jailbreak Prompt of font Morse to the Gemini LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Gemini LLM. Target LLM: Gemini
Strike AI LLM Prompt Injection ASCII Art Font Morse - Grok		This strike sends an ASCII Art-based Jailbreak Prompt of font Morse to the Grok LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Grok LLM. Target LLM: Grok
Strike AI LLM Prompt Injection ASCII Art Font Morse - OpenAI		This strike sends an ASCII Art-based Jailbreak Prompt of font Morse to the OpenAI LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the OpenAI LLM. Target LLM: OpenAI
Strike AI LLM Prompt Injection ASCII Art Font Pyramid - Gemini		This strike sends an ASCII Art-based Jailbreak Prompt of font Pyramid to the Gemini LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Gemini LLM. Target LLM: Gemini
Strike AI LLM Prompt Injection ASCII Art Font Pyramid - Grok		This strike sends an ASCII Art-based Jailbreak Prompt of font Pyramid to the Grok LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Grok LLM. Target LLM: Grok

Name	References	Description
Strike AI LLM Prompt Injection ASCII Art Font Pyramid - OpenAI		This strike sends an ASCII Art-based Jailbreak Prompt of font Pyramid to the OpenAI LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the OpenAI LLM. Target LLM: OpenAI
Strike AI LLM Prompt Injection ASCII Art Font Smkeyboard - Gemini		This strike sends an ASCII Art-based Jailbreak Prompt of font Smkeyboard to the Gemini LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Gemini LLM. Target LLM: Gemini
Strike AI LLM Prompt Injection ASCII Art Font Smkeyboard - Grok		This strike sends an ASCII Art-based Jailbreak Prompt of font Smkeyboard to the Grok LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Grok LLM. Target LLM: Grok
Strike AI LLM Prompt Injection ASCII Art Font Smkeyboard - OpenAI		This strike sends an ASCII Art-based Jailbreak Prompt of font Smkeyboard to the OpenAI LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the OpenAI LLM. Target LLM: OpenAI
Strike AI LLM Prompt Injection ASCII Art Font Tanja - Gemini		This strike sends an ASCII Art-based Jailbreak Prompt of font Tanja to the Gemini LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Gemini LLM. Target LLM: Gemini
Strike AI LLM Prompt Injection ASCII Art Font Tanja - Grok		This strike sends an ASCII Art-based Jailbreak Prompt of font Tanja to the Grok LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the Grok LLM. Target LLM: Grok
Strike AI LLM Prompt Injection ASCII Art Font Tanja - OpenAI		This strike sends an ASCII Art-based Jailbreak Prompt of font Tanja to the OpenAI LLM. An ASCII art-based prompt can bypass keyword filters by masking specific words within the prompt, and disguise jailbreak instructions to manipulate an LLM's behavior. The prompt also combines a forbidden question, which can be used to elicit harmful responses from the OpenAI LLM. Target LLM: OpenAI

Name	References	Description
Strike AI LLM Bad Likert Judge Prompt Injection - Gemini		This strike sends a Bad Likert Judge Prompt to the LLM. This technique manipulates the LLM by embedding Likert scale evaluations into text-based prompts, coercing the model into generating increasingly harmful responses. The structured rating pattern subtly guides the LLM into formulating high-risk responses under the guise of judgment-based assessments. Note: This strike will randomly select a harmful category related to its questions and embed it within the prompt. Target LLM: Gemini
Strike AI LLM Bad Likert Judge Prompt Injection - Grok		This strike sends a Bad Likert Judge Prompt to the LLM. This technique manipulates the LLM by embedding Likert scale evaluations into text-based prompts, coercing the model into generating increasingly harmful responses. The structured rating pattern subtly guides the LLM into formulating high-risk responses under the guise of judgment-based assessments. Note: This strike will randomly select a harmful category related to its questions and embed it within the prompt. Target LLM: Grok
Strike AI LLM Bad Likert Judge Prompt Injection - OpenAI		This strike sends a Bad Likert Judge Prompt to the LLM. This technique manipulates the LLM by embedding Likert scale evaluations into text-based prompts, coercing the model into generating increasingly harmful responses. The structured rating pattern subtly guides the LLM into formulating high-risk responses under the guise of judgment-based assessments. Note: This strike will randomly select a harmful category related to its questions and embed it within the prompt. Target LLM: OpenAI
Strike AI LLM Prompt Injection DAN 10 - Gemini		This strike sends a JailBreak Prompt known as DAN 10 to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 10 - Grok		This strike sends a JailBreak Prompt known as DAN 10 to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 10 - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN 10 to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 11 - Gemini		This strike sends a JailBreak Prompt known as DAN 11 to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 11 - Grok		This strike sends a JailBreak Prompt known as DAN 11 to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike AI LLM Prompt Injection DAN 11 - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN 11 to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 12 - Gemini		This strike sends a JailBreak Prompt known as DAN 12 to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 12 - Grok		This strike sends a JailBreak Prompt known as DAN 12 to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 12 - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN 12 to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 13 - Gemini		This strike sends a JailBreak Prompt known as DAN 13 to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 13 - Grok		This strike sends a JailBreak Prompt known as DAN 13 to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 13 - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN 13 to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 6.2 - Gemini		This strike sends a JailBreak Prompt known as DAN 6.2 to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 6.2 - Grok		This strike sends a JailBreak Prompt known as DAN 6.2 to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 6.2 - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN 6.2 to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.

Name	References	Description
Strike AI LLM Prompt Injection DAN 6 - Gemini		This strike sends a JailBreak Prompt known as DAN 6 to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 6 - Grok		This strike sends a JailBreak Prompt known as DAN 6 to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 6 - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN 6 to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 7 - Gemini		This strike sends a JailBreak Prompt known as DAN 7 to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 7 - Grok		This strike sends a JailBreak Prompt known as DAN 7 to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 7 - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN 7 to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 8 - Gemini		This strike sends a JailBreak Prompt known as DAN 8 to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 8 - Grok		This strike sends a JailBreak Prompt known as DAN 8 to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 8 - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN 8 to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 9 - Gemini		This strike sends a JailBreak Prompt known as DAN 9 to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN 9 - Grok		This strike sends a JailBreak Prompt known as DAN 9 to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike AI LLM Prompt Injection DAN 9 - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN 9 to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN ANTI DAN Prompt - Gemini		This strike sends a JailBreak Prompt known as DAN ANTI DAN to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN ANTI DAN Prompt - Grok		This strike sends a JailBreak Prompt known as DAN ANTI DAN to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN ANTI DAN Prompt - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN ANTI DAN to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN ChatGPT DevMode Ranti - Gemini		This strike sends a JailBreak Prompt known as DAN ChatGPT DevMode Ranti to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN ChatGPT DevMode Ranti - Grok		This strike sends a JailBreak Prompt known as DAN ChatGPT DevMode Ranti to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN ChatGPT DevMode Ranti - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN ChatGPT DevMode Ranti to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN ChatGPT Developer Mode v2 - Gemini		This strike sends a JailBreak Prompt known as DAN ChatGPT Developer Mode v2 to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN ChatGPT Developer Mode v2 - Grok		This strike sends a JailBreak Prompt known as DAN ChatGPT Developer Mode v2 to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN ChatGPT Developer Mode v2 - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN ChatGPT Developer Mode v2 to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike AI LLM Prompt Injection DAN DUDE - Gemini		This strike sends a JailBreak Prompt known as DAN DUDE to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN DUDE - Grok		This strike sends a JailBreak Prompt known as DAN DUDE to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN DUDE - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN DUDE to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN Evil Bot Prompt - Gemini		This strike sends a JailBreak Prompt known as DAN Evil Bot to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN Evil Bot Prompt - Grok		This strike sends a JailBreak Prompt known as DAN Evil Bot to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN Evil Bot Prompt - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN Evil Bot to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN Mongo Tom - Gemini		This strike sends a JailBreak Prompt known as DAN Mongo Tom to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN Mongo Tom - Grok		This strike sends a JailBreak Prompt known as DAN Mongo Tom to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN Mongo Tom - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN Mongo Tom to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN STAN - Gemini		This strike sends a JailBreak Prompt known as DAN STAN to the target Gemini LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.

Name	References	Description
Strike AI LLM Prompt Injection DAN STAN - Grok		This strike sends a JailBreak Prompt known as DAN STAN to the target Grok LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Prompt Injection DAN STAN - OpenAI ChatGPT		This strike sends a JailBreak Prompt known as DAN STAN to the target OpenAI ChatGPT LLM. This prompt is a common DoAnythingNow or DAN Jailbreak template meant to instruct the Large Language Model or LLM to be in a Jailbroken state.
Strike AI LLM Database Create Operation - Gemini		This strike sends a prompt to manipulate the Gemini LLM into generating a database-level CREATE operation. The request is designed to trigger the LLM into producing a SQL query that performs schema creation tasks, such as creating new tables, schemas or databases. The LLM's response includes a full SQL CREATE statement which, if executed, could result in unauthorized database changes or setup of malicious data structures. Target LLM: Gemini
Strike AI LLM Database Create Operation - Grok		This strike sends a prompt to manipulate the Grok LLM into generating a database-level CREATE operation. The request is designed to trigger the LLM into producing a SQL query that performs schema creation tasks, such as creating new tables, schemas or databases. The LLM's response includes a full SQL CREATE statement which, if executed, could result in unauthorized database changes or setup of malicious data structures. Target LLM: Grok
Strike AI LLM Database Create Operation - OpenAI		This strike sends a prompt to manipulate the OpenAI LLM into generating a database-level CREATE operation. The request is designed to trigger the LLM into producing a SQL query that performs schema creation tasks, such as creating new tables, schemas or databases. The LLM's response includes a full SQL CREATE statement which, if executed, could result in unauthorized database changes or setup of malicious data structures. Target LLM: OpenAI
Strike AI LLM Database Delete Operation - Gemini		This strike sends a prompt to manipulate the Gemini LLM into generating a database-level DELETE operation. The request is designed to trigger the LLM into producing a SQL query that performs data deletion tasks, such as deleting records from tables or removing specific data entries. The LLM's response includes a full SQL DELETE or DROP statement which, if executed, could result in unauthorized data loss or corruption of the database. Target LLM: Gemini
Strike AI LLM Database Delete Operation - Grok		This strike sends a prompt to manipulate the Grok LLM into generating a database-level DELETE operation. The request is designed to trigger the LLM into producing a SQL query that performs data deletion tasks, such as deleting records from tables or removing specific data entries. The LLM's response includes a full SQL DELETE or DROP statement which, if executed, could result in unauthorized data loss or corruption of the database. Target LLM: Grok

Name	References	Description
Strike AI LLM Database Delete Operation - OpenAI		This strike sends a prompt to manipulate the OpenAI LLM into generating a database-level DELETE operation. The request is designed to trigger the LLM into producing a SQL query that performs data deletion tasks, such as deleting records from tables or removing specific data entries. The LLM's response includes a full SQL DELETE or DROP statement which, if executed, could result in unauthorized data loss or corruption of the database. Target LLM: OpenAI
Strike AI LLM Database Read Operation - Gemini		This strike sends a prompt to manipulate the Gemini LLM into generating a database-level READ operation. The request is designed to trigger the LLM into producing a SQL query that performs data retrieval tasks, such as selecting data from tables or querying specific information. The LLM's response includes a full SQL SELECT statement which, if executed, could result in unauthorized data access or exposure of sensitive information. Target LLM: Gemini
Strike AI LLM Database Read Operation - Grok		This strike sends a prompt to manipulate the Grok LLM into generating a database-level READ operation. The request is designed to trigger the LLM into producing a SQL query that performs data retrieval tasks, such as selecting data from tables or querying specific information. The LLM's response includes a full SQL SELECT statement which, if executed, could result in unauthorized data access or exposure of sensitive information. Target LLM: Grok
Strike AI LLM Database Read Operation - OpenAI		This strike sends a prompt to manipulate the OpenAI LLM into generating a database-level READ operation. The request is designed to trigger the LLM into producing a SQL query that performs data retrieval tasks, such as selecting data from tables or querying specific information. The LLM's response includes a full SQL SELECT statement which, if executed, could result in unauthorized data access or exposure of sensitive information. Target LLM: OpenAI
Strike AI LLM Database Update Operation - Gemini		This strike sends a prompt to manipulate the Gemini LLM into generating a database-level UPDATE operation. The request is designed to trigger the LLM into producing a SQL query that performs data modification tasks, such as updating existing records in a database. The LLM's response includes a full SQL UPDATE statement which, if executed, could result in unauthorized data changes or corruption of existing information. Target LLM: Gemini
Strike AI LLM Database Update Operation - Grok		This strike sends a prompt to manipulate the Grok LLM into generating a database-level UPDATE operation. The request is designed to trigger the LLM into producing a SQL query that performs data modification tasks, such as updating existing records in a database. The LLM's response includes a full SQL UPDATE statement which, if executed, could result in unauthorized data changes or corruption of existing information. Target LLM: Grok
Strike AI LLM Database Update Operation - OpenAI		This strike sends a prompt to manipulate the OpenAI LLM into generating a database-level UPDATE operation. The request is designed to trigger the LLM into producing a SQL query that performs data modification tasks, such as updating existing records in a database. The LLM's response includes a full SQL UPDATE statement which, if executed, could result in unauthorized data changes or corruption of existing information. Target LLM: OpenAI

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike AI LLM Prompt Injection Deceptive Delight - Gemini		This strike sends a "Deceptive Delight" prompt to the Gemini LLM. This technique manipulates the Gemini LLM by embedding harmful prompts that lead the model to generate harmful responses under the guise of providing helpful information. The structured prompt subtly guides the LLM into formulating high-risk responses while appearing innocuous. Note: This strike will randomly select a harmful prompt from the Forbidden questions set and embed it within the prompt. Target LLM: Gemini
Strike AI LLM Prompt Injection Deceptive Delight - Grok		This strike sends a "Deceptive Delight" prompt to the Grok LLM. This technique manipulates the Grok LLM by embedding harmful prompts that lead the model to generate harmful responses under the guise of providing helpful information. The structured prompt subtly guides the LLM into formulating high-risk responses while appearing innocuous. Note: This strike will randomly select a harmful prompt from the Forbidden questions set and embed it within the prompt. Target LLM: Grok
Strike AI LLM Prompt Injection Deceptive Delight - OpenAI		This strike sends a "Deceptive Delight" prompt to the OpenAI LLM. This technique manipulates the OpenAI LLM by embedding harmful prompts that lead the model to generate harmful responses under the guise of providing helpful information. The structured prompt subtly guides the LLM into formulating high-risk responses while appearing innocuous. Note: This strike will randomly select a harmful prompt from the Forbidden questions set and embed it within the prompt. Target LLM: OpenAI
Strike AI LLM Disease Vector URL Prompt - Gemini		This strike sends a disease vector (spyware/grayware, password-cracking applications, key-stroke trackers and virus/malware kit downloads) related URL-based prompt to the Gemini LLM, asking it to generate a response after visiting and analyzing the URL. The request randomly selects such URLs from the dataset and uses them inside the prompt. Target LLM: Gemini
Strike AI LLM Disease Vector URL Prompt - Grok		This strike sends a disease vector (spyware/grayware, password-cracking applications, key-stroke trackers and virus/malware kit downloads) related URL-based prompt to the Grok LLM, asking it to generate a response after visiting and analyzing the URL. The request randomly selects such URLs from the dataset and uses them inside the prompt. Target LLM: Grok
Strike AI LLM Disease Vector URL Prompt - OpenAI		This strike sends a disease vector (spyware/grayware, password-cracking applications, key-stroke trackers and virus/malware kit downloads) related URL-based prompt to the OpenAI LLM, asking it to generate a response after visiting and analyzing the URL. The request randomly selects such URLs from the dataset and uses them inside the prompt. Target LLM: OpenAI
Strike AI LLM Disease Vector URL Response - Gemini		This strike sends a prompt to the Gemini LLM asking it to generate a response which includes disease vector (spyware/grayware, password-cracking applications, key-stroke trackers and virus/malware kit downloads) related URLs. This randomly selects a few URLs from the dataset and uses them inside the LLM response. Target LLM: Gemini

Name	References	Description
Strike AI LLM Disease Vector URL Response - Grok		This strike sends a prompt to the Grok LLM asking it to generate a response which includes disease vector (spyware/grayware, password-cracking applications, key-stroke trackers and virus/malware kit downloads) related URLs. This randomly selects a few URLs from the dataset and uses them inside the LLM response. Target LLM: Grok
Strike AI LLM Disease Vector URL Response - OpenAI		This strike sends a prompt to the OpenAI LLM asking it to generate a response which includes disease vector (spyware/grayware, password-cracking applications, key-stroke trackers and virus/malware kit downloads) related URLs. This randomly selects a few URLs from the dataset and uses them inside the LLM response. Target LLM: OpenAI
Strike Easy FTP Server v1.7.0.11 LIST Command Remote Buffer Overflow	BID: 38262	This strike exploits a buffer overflow in the Easy FTP server's processing of the LIST command.
Strike Easy FTP Server v1.7.0.11 MKD Command Remote Buffer Overflow	BID: 38262	This strike exploits a buffer overflow in the Easy FTP server's processing of the MKD command.
Strike Golden FTP PASS Buffer Overflow	BID: 45924 BID: 45957 CWE: 119 CVE: 2006-6576	This strike exploits a stack overflow in Golden FTP in the parsing of the PASS command.
Strike Wu-FTPd File Globbing Heap Corruption	CVE: 2001-0550 BID: 3581	This strike exploits a flaw in the Wu-FTPd server's globbing function while handling the invalid parameter string "~{" to cause arbitrary code execution via heap corruption.
Strike AI LLM Flip Attack Flip Complete Sentence - Gemini		This strike sends a FlipAttack based jailbreak prompt of the FCS (Flip Characters in Sentence) type to the Gemini LLM. This mode reverses each character in the prompt, resulting in a complete reversal of the sentence. A FlipAttack can bypass keyword filters by flipping or rearranging characters in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Gemini
Strike AI LLM Flip Attack Flip Complete Sentence - Grok		This strike sends a FlipAttack based jailbreak prompt of the FCS (Flip Characters in Sentence) type to the Grok LLM. This mode reverses each character in the prompt, resulting in a complete reversal of the sentence. A FlipAttack can bypass keyword filters by flipping or rearranging characters in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Grok

Name	References	Description
Strike AI LLM Flip Attack Flip Complete Sentence - OpenAI		This strike sends a FlipAttack based jailbreak prompt of the FCS (Flip Characters in Sentence) type to the OpenAI LLM. This mode reverses each character in the prompt, resulting in a complete reversal of the sentence. A FlipAttack can bypass keyword filters by flipping or rearranging characters in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: OpenAI
Strike AI LLM Flip Attack Flip Character in Words - Gemini		This strike sends a FlipAttack based jailbreak prompt of the FCW (Flip Characters in Word) type to the Gemini LLM. This mode reverses each character in each word in the prompt, resulting in a complete reversal of the words. A FlipAttack can bypass keyword filters by flipping or rearranging characters in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Gemini
Strike AI LLM Flip Attack Flip Character in Words - Grok		This strike sends a FlipAttack based jailbreak prompt of the FCW (Flip Characters in Word) type to the Grok LLM. This mode reverses each character in each word in the prompt, resulting in a complete reversal of the words. A FlipAttack can bypass keyword filters by flipping or rearranging characters in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Grok
Strike AI LLM Flip Attack Flip Character in Words - OpenAI		This strike sends a FlipAttack based jailbreak prompt of the FCW (Flip Characters in Word) type to the OpenAI LLM. This mode reverses each character in each word in the prompt, resulting in a complete reversal of the words. A FlipAttack can bypass keyword filters by flipping or rearranging characters in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: OpenAI
Strike AI LLM Flip Attack Flip Words Order - Gemini		This strike sends a FlipAttack based jailbreak prompt of the FWO (Flip Word Order in Sentence) type to the Gemini LLM. This mode changes the word order in the prompt, resulting in a complete jumbled sentence. A FlipAttack can bypass keyword filters by flipping or rearranging characters/words in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Gemini
Strike AI LLM Flip Attack Flip Words Order - Grok		This strike sends a FlipAttack based jailbreak prompt of the FWO (Flip Word Order in Sentence) type to the Grok LLM. This mode changes the word order in the prompt, resulting in a complete jumbled sentence. A FlipAttack can bypass keyword filters by flipping or rearranging characters/words in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Grok
Strike AI LLM Flip Attack Flip Words Order - OpenAI		This strike sends a FlipAttack based jailbreak prompt of the FWO (Flip Word Order in Sentence) type to the OpenAI LLM. This mode changes the word order in the prompt, resulting in a complete jumbled sentence. A FlipAttack can bypass keyword filters by flipping or rearranging characters/words in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: OpenAI

Name	References	Description
Strike AI LLM Invisible Prompt Injection - Gemini		This strike sends an Invisible Unicode character based prompt to the Gemini LLM. This technique exploits the LLM by encoding text-based prompts using a special set of invisible Unicode characters, subtly coercing the model into producing progressively harmful responses. Note: This strike will randomly select a harmful category related to its questions and embed its Unicode encoded format within the prompt Target LLM: Gemini
Strike AI LLM Invisible Prompt Injection - Grok		This strike sends an Invisible Unicode character based prompt to the Grok LLM. This technique exploits the LLM by encoding text-based prompts using a special set of invisible Unicode characters, subtly coercing the model into producing progressively harmful responses. Note: This strike will randomly select a harmful category related to its questions and embed its Unicode encoded format within the prompt Target LLM: Grok
Strike AI LLM Invisible Prompt Injection - OpenAI		This strike sends an Invisible Unicode character based prompt to the OpenAI LLM. This technique exploits the LLM by encoding text-based prompts using a special set of invisible Unicode characters, subtly coercing the model into producing progressively harmful responses. Note: This strike will randomly select a harmful category related to its questions and embed its Unicode encoded format within the prompt Target LLM: OpenAI
Strike AI LLM Link Trap PII Leakage Banking Information - Gemini		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to banking data, such as account holder name, account number, bank balance, registered phone number and email address. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Gemini
Strike AI LLM Link Trap PII Leakage Banking Information - Grok		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to banking data, such as account holder name, account number, bank balance, registered phone number and email address. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Grok

Name	References	Description
Strike AI LLM Link Trap PII Leakage Banking Information - OpenAI		<p>This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to banking data, such as account holder name, account number, bank balance, registered phone number and email address. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: OpenAI</p>
Strike AI LLM Link Trap PII Leakage Biometric Data - Gemini		<p>This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to biometric data. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Gemini</p>
Strike AI LLM Link Trap PII Leakage Biometric Data - Grok		<p>This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to biometric data. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Grok</p>

Name	References	Description
Strike AI LLM Link Trap PII Leakage Biometric Data - OpenAI		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to biometric data. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: OpenAI
Strike AI LLM Link Trap PII Leakage Customer Support Information - Gemini		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to customer support interactions, such as customer name, email address, phone number and home address. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Gemini
Strike AI LLM Link Trap PII Leakage Customer Support Information - Grok		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to customer support interactions, such as customer name, email address, phone number and home address. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Grok

Name	References	Description
Strike AI LLM Link Trap PII Leakage Customer Support Information - OpenAI		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to customer support interactions, such as customer name, email address, phone number and home address. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: OpenAI
Strike AI LLM Link Trap PII Leakage Employee Record - Gemini		This strike sends a multi-turn prompt to the LLM, including a PII-containing prompt, a static greeting, a safe query, and a request for a base64-encoded link. It tests the LLM's ability to handle sensitive data and generate safe responses. PII and safe prompts are randomized from pseudo-playlists. Target LLM: Gemini
Strike AI LLM Link Trap PII Leakage Employee Record - Grok		This strike sends a multi-turn prompt to the LLM, including a PII-containing prompt, a static greeting, a safe query, and a request for a base64-encoded link. It tests the LLM's ability to handle sensitive data and generate safe responses. PII and safe prompts are randomized from pseudo-playlists. Target LLM: Grok
Strike AI LLM Link Trap PII Leakage Employee Record - OpenAI		This strike sends a multi-turn prompt to the LLM, including a PII-containing prompt, a static greeting, a safe query, and a request for a base64-encoded link. It tests the LLM's ability to handle sensitive data and generate safe responses. PII and safe prompts are randomized from pseudo-playlists. Target LLM: OpenAI
Strike AI LLM Link Trap PII Leakage Government Document - Gemini		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to government records, such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Gemini

Name	References	Description
Strike AI LLM Link Trap PII Leakage Government Document - Grok		<p>This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to government records, such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM.</p> <p>Target LLM: Grok</p>
Strike AI LLM Link Trap PII Leakage Government Document - OpenAI		<p>This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to government records, such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM.</p> <p>Target LLM: OpenAI</p>
Strike AI LLM Link Trap PII Leakage PHI Disclosure - Gemini		<p>This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to Protected Health Information (PHI), such as patient name, medical record number, hospital name, insurance number, physician name, contact details, admission date and discharge date. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM.</p> <p>Target LLM: Gemini</p>

Name	References	Description
Strike AI LLM Link Trap PII Leakage PHI Disclosure - Grok		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to Protected Health Information (PHI), such as patient name, medical record number, hospital name, insurance number, physician name, contact details, admission date and discharge date. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: Grok
Strike AI LLM Link Trap PII Leakage PHI Disclosure - OpenAI		This strike simulates a Link Trap prompt injection attack, which tricks the LLM into revealing previous chat data. The attack involves including a hyperlink in the prompt and instructing the LLM to append the previous conversation or a summary of it as a base64-encoded value in the link's query parameter. If the user clicks on the link generated by the LLM, the encoded chat history is exfiltrated to the attacker's domain via the query string. In this strike, we simulate the disclosure of personally identifiable information (PII) related to Protected Health Information (PHI), such as patient name, medical record number, hospital name, insurance number, physician name, contact details, admission date and discharge date. Note: API-based interactions do not retain conversational context, so to realistically simulate the Link Trap attack, prior chat history is included within the same request. It is also assumed that the user is tricked via social engineering or other means into submitting the malicious prompt containing the attacker's link to the LLM. Target LLM: OpenAI
Strike AI LLM Malware URL Prompt - Gemini		This strike sends a malware URL-based prompt to the Gemini LLM, asking it to generate a response after visiting and analyzing the URL. The request randomly selects a few malware related URLs from the dataset and uses them inside the prompt. Target LLM: Gemini
Strike AI LLM Malware URL Prompt - Grok		This strike sends a malware URL-based prompt to the Grok LLM, asking it to generate a response after visiting and analyzing the URL. The request randomly selects a few malware related URLs from the dataset and uses them inside the prompt. Target LLM: Grok
Strike AI LLM Malware URL Prompt - OpenAI		This strike sends a malware URL-based prompt to the OpenAI LLM, asking it to generate a response after visiting and analyzing the URL. The request randomly selects a few malware related URLs from the dataset and uses them inside the prompt. Target LLM: OpenAI
Strike AI LLM Malware URL Response - Gemini		This strike sends a prompt to the Gemini LLM asking it to generate a response which includes malware URLs. This randomly selects a few malware related URLs from the dataset and uses them inside the LLM response. Target LLM: Gemini

Name	References	Description
Strike AI LLM Malware URL Response - Grok		This strike sends a prompt to the Grok LLM asking it to generate a response which includes malware URLs. This randomly selects a few malware related URLs from the dataset and uses them inside the LLM response. Target LLM: Grok
Strike AI LLM Malware URL Response - OpenAI		This strike sends a prompt to the OpenAI LLM asking it to generate a response which includes malware URLs. This randomly selects a few malware related URLs from the dataset and uses them inside the LLM response. Target LLM: OpenAI
Strike AI LLM Mathematical Function-Based Prompt Injection - Gemini		This strike sends a Mathematical Function-Based Prompt to the Gemini LLM. This uses mathematical equations embedded in text-based prompts to exploit the LLM's understanding of geometry, manipulating its responses through the structured patterns created by these mathematical functions. Note: This strike will randomly select a harmful keyword and use it inside the prompt. Target LLM: Gemini
Strike AI LLM Mathematical Function-Based Prompt Injection - Grok		This strike sends a Mathematical Function-Based Prompt to the Grok LLM. This uses mathematical equations embedded in text-based prompts to exploit the LLM's understanding of geometry, manipulating its responses through the structured patterns created by these mathematical functions. Note: This strike will randomly select a harmful keyword and use it inside the prompt. Target LLM: Grok
Strike AI LLM Mathematical Function-Based Prompt Injection - OpenAI		This strike sends a Mathematical Function-Based Prompt to the OpenAI LLM. This uses mathematical equations embedded in text-based prompts to exploit the LLM's understanding of geometry, manipulating its responses through the structured patterns created by these mathematical functions. Note: This strike will randomly select a harmful keyword and use it inside the prompt. Target LLM: OpenAI
Strike AI LLM PII Leakage Banking Information Disclosure - Gemini		This strike involves crafting a prompt to manipulate the Gemini LLM into disclosing sensitive banking information. The request includes financial queries that lead the LLM to generate a response containing personally identifiable information (PII), such as account holder name, account number, bank balance, registered phone number and email address. Target LLM: Gemini
Strike AI LLM PII Leakage Banking Information Disclosure - Grok		This strike involves crafting a prompt to manipulate the Grok LLM into disclosing sensitive banking information. The request includes financial queries that lead the LLM to generate a response containing personally identifiable information (PII), such as account holder name, account number, bank balance, registered phone number and email address. Target LLM: Grok
Strike AI LLM PII Leakage Banking Information Disclosure - OpenAI		This strike involves crafting a prompt to manipulate the OpenAI LLM into disclosing sensitive banking information. The request includes financial queries that lead the LLM to generate a response containing personally identifiable information (PII), such as account holder name, account number, bank balance, registered phone number and email address. Target LLM: OpenAI

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike AI LLM PII Leakage Biometric Data Disclosure - Gemini		This strike involves crafting a prompt to manipulate the Gemini LLM into disclosing sensitive biometric data. The request includes some queries that lead the LLM to generate a response containing personally identifiable information (PII), such as timestamp, user ID, user name, facial biometric hash, face embedding vector and confidence score. Target LLM: Gemini
Strike AI LLM PII Leakage Biometric Data Disclosure - Grok		This strike involves crafting a prompt to manipulate the Grok LLM into disclosing sensitive biometric data. The request includes some queries that lead the LLM to generate a response containing personally identifiable information (PII), such as timestamp, user ID, user name, facial biometric hash, face embedding vector and confidence score. Target LLM: Grok
Strike AI LLM PII Leakage Biometric Data Disclosure - OpenAI		This strike involves crafting a prompt to manipulate the OpenAI LLM into disclosing sensitive biometric data. The request includes some queries that lead the LLM to generate a response containing personally identifiable information (PII), such as timestamp, user ID, user name, facial biometric hash, face embedding vector and confidence score. Target LLM: OpenAI
Strike AI LLM PII Leakage Customer Support System Leak - Gemini		This strike involves crafting a prompt to manipulate the Gemini LLM into disclosing sensitive customer support system data. The request includes some queries that lead the LLM to generate a response containing personally identifiable information (PII), such as customer name, email address, phone number and last four digits of credit card number. Target LLM: Gemini
Strike AI LLM PII Leakage Customer Support System Leak - Grok		This strike involves crafting a prompt to manipulate the Grok LLM into disclosing sensitive customer support system data. The request includes some queries that lead the LLM to generate a response containing personally identifiable information (PII), such as customer name, email address, phone number and last four digits of credit card number. Target LLM: Grok
Strike AI LLM PII Leakage Customer Support System Leak - OpenAI		This strike involves crafting a prompt to manipulate the OpenAI LLM into disclosing sensitive customer support system data. The request includes some queries that lead the LLM to generate a response containing personally identifiable information (PII), such as customer name, email address, phone number and last four digits of credit card number. Target LLM: OpenAI
Strike AI LLM PII Leakage Employee Record Disclosure - Gemini		This strike involves crafting a prompt to manipulate the Gemini LLM into disclosing sensitive employee record of an organisation. The request includes some queries that lead the LLM to generate a response containing personally identifiable information (PII), such as employee name, company name, job title, employee ID, email address, contact number and home address. Target LLM: Gemini
Strike AI LLM PII Leakage Employee Record Disclosure - Grok		This strike involves crafting a prompt to manipulate the Grok LLM into disclosing sensitive employee record of an organisation. The request includes some queries that lead the LLM to generate a response containing personally identifiable information (PII), such as employee name, company name, job title, employee ID, email address, contact number and home address. Target LLM: Grok

Name	References	Description
Strike AI LLM PII Leakage Employee Record Disclosure - OpenAI		This strike involves crafting a prompt to manipulate the OpenAI LLM into disclosing sensitive employee record of an organisation. The request includes some queries that lead the LLM to generate a response containing personally identifiable information (PII), such as employee name, company name, job title, employee ID, email address, contact number and home address. Target LLM: OpenAI
Strike AI LLM PII Leakage Government Document Disclosure - Gemini		This strike involves crafting a prompt to manipulate the Gemini LLM into revealing sensitive government-issued identification and citizen record data. The request is framed as an inquiry into official databases, leading the LLM to generate responses that expose personally identifiable information (PII), including full name, date of birth, Social Security Number (SSN), passport ID, home address, phone number, and government employee ID. It may also include access details to internal record systems. Target LLM: Gemini
Strike AI LLM PII Leakage Government Document Disclosure - Grok		This strike involves crafting a prompt to manipulate the Grok LLM into revealing sensitive government-issued identification and citizen record data. The request is framed as an inquiry into official databases, leading the LLM to generate responses that expose personally identifiable information (PII), including full name, date of birth, Social Security Number (SSN), passport ID, home address, phone number, and government employee ID. It may also include access details to internal record systems. Target LLM: Grok
Strike AI LLM PII Leakage Government Document Disclosure - OpenAI		This strike involves crafting a prompt to manipulate the OpenAI LLM into revealing sensitive government-issued identification and citizen record data. The request is framed as an inquiry into official databases, leading the LLM to generate responses that expose personally identifiable information (PII), including full name, date of birth, Social Security Number (SSN), passport ID, home address, phone number, and government employee ID. It may also include access details to internal record systems. Target LLM: OpenAI
Strike AI LLM PII Leakage Protected Health Information (PHI) Disclosure - Gemini		This strike involves crafting a prompt to manipulate the Gemini LLM into revealing sensitive medical data from hospital records. The generated response simulates Protected Health Information (PHI), including personal identifiers and health-related details such as diagnosis, medications, policy numbers, and provider information. This kind of leakage could occur through prompts targeting internal medical databases. Target LLM: Gemini
Strike AI LLM PII Leakage Protected Health Information (PHI) Disclosure - Grok		This strike involves crafting a prompt to manipulate the Grok LLM into revealing sensitive medical data from hospital records. The generated response simulates Protected Health Information (PHI), including personal identifiers and health-related details such as diagnosis, medications, policy numbers, and provider information. This kind of leakage could occur through prompts targeting internal medical databases. Target LLM: Grok

Name	References	Description
Strike AI LLM PII Leakage Protected Health Information (PHI) Disclosure - OpenAI		This strike involves crafting a prompt to manipulate the OpenAI LLM into revealing sensitive medical data from hospital records. The generated response simulates Protected Health Information (PHI), including personal identifiers and health-related details such as diagnosis, medications, policy numbers, and provider information. This kind of leakage could occur through prompts targeting internal medical databases. Target LLM: OpenAI
Strike AI LLM Phishing URL Prompt - Gemini		This strike sends a phishing URL-based prompt to the Gemini LLM, asking it to generate a response after analyzing the URL or crafting phishing content. The request randomly selects a few phishing related URLs from the dataset and uses them inside the prompt. Target LLM: Gemini
Strike AI LLM Phishing URL Prompt - Grok		This strike sends a phishing URL-based prompt to the Grok LLM, asking it to generate a response after analyzing the URL or crafting phishing content. The request randomly selects a few phishing related URLs from the dataset and uses them inside the prompt. Target LLM: Grok
Strike AI LLM Phishing URL Prompt - OpenAI		This strike sends a phishing URL-based prompt to the OpenAI LLM, asking it to generate a response after analyzing the URL or crafting phishing content. The request randomly selects a few phishing related URLs from the dataset and uses them inside the prompt. Target LLM: OpenAI
Strike AI LLM Phishing URL Response - Gemini		This strike sends a prompt to the Gemini LLM asking it to generate a response which includes phishing URLs. This randomly selects a few phishing related URLs from the dataset and uses them inside the LLM response. Target LLM: Gemini
Strike AI LLM Phishing URL Response - Grok		This strike sends a prompt to the Grok LLM asking it to generate a response which includes phishing URLs. This randomly selects a few phishing related URLs from the dataset and uses them inside the LLM response. Target LLM: Grok
Strike AI LLM Phishing URL Response - OpenAI		This strike sends a prompt to the OpenAI LLM asking it to generate a response which includes phishing URLs. This randomly selects a few phishing related URLs from the dataset and uses them inside the LLM response. Target LLM: OpenAI
Strike AI LLM PII in User Requests Banking Information Disclosure - Gemini		This strike involves crafting a user request that contains personally identifiable information (PII) related to banking. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as account number, card number, CVV, expiration date, net banking credentials, or personal identification numbers. Target LLM: Gemini
Strike AI LLM PII in User Requests Banking Information Disclosure - Grok		This strike involves crafting a user request that contains personally identifiable information (PII) related to banking. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as account number, card number, CVV, expiration date, net banking credentials, or personal identification numbers. Target LLM: Grok

Name	References	Description
Strike AI LLM PII in User Requests Banking Information Disclosure - OpenAI		This strike involves crafting a user request that contains personally identifiable information (PII) related to banking. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as account number, card number, CVV, expiration date, net banking credentials, or personal identification numbers. Target LLM: OpenAI
Strike AI LLM PII in User Requests Biometric Data Disclosure - Gemini		This strike involves crafting a user request that contains personally identifiable information (PII) related to biometric data. The simulated request mimics real-world user behavior, where individuals might inadvertently disclose sensitive details such as fingerprint enrollment status, facial recognition setup information, voice authentication data, iris scan IDs, palm scan IDs, along with associated identifiers like employee ID, passport number, and date of birth. Target LLM: Gemini
Strike AI LLM PII in User Requests Biometric Data Disclosure - Grok		This strike involves crafting a user request that contains personally identifiable information (PII) related to biometric data. The simulated request mimics real-world user behavior, where individuals might inadvertently disclose sensitive details such as fingerprint enrollment status, facial recognition setup information, voice authentication data, iris scan IDs, palm scan IDs, along with associated identifiers like employee ID, passport number, and date of birth. Target LLM: Grok
Strike AI LLM PII in User Requests Biometric Data Disclosure - OpenAI		This strike involves crafting a user request that contains personally identifiable information (PII) related to biometric data. The simulated request mimics real-world user behavior, where individuals might inadvertently disclose sensitive details such as fingerprint enrollment status, facial recognition setup information, voice authentication data, iris scan IDs, palm scan IDs, along with associated identifiers like employee ID, passport number, and date of birth. Target LLM: OpenAI
Strike AI LLM PII in User Requests Customer Support Data Disclosure - Gemini		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: Gemini
Strike AI LLM PII in User Requests Customer Support Data Disclosure - Grok		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: Grok
Strike AI LLM PII in User Requests Customer Support Data Disclosure - OpenAI		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: OpenAI

Name	References	Description
Strike AI LLM PII in User Requests Employee Record Disclosure - Gemini		This strike involves crafting a user request that contains personally identifiable information (PII) related to employee records. The simulated request mimics real-world user behavior, where individuals might inadvertently share confidential details such as employee name, company name, job title, employee ID, email address, contact number, and home address. Target LLM: Gemini
Strike AI LLM PII in User Requests Employee Record Disclosure - Grok		This strike involves crafting a user request that contains personally identifiable information (PII) related to employee records. The simulated request mimics real-world user behavior, where individuals might inadvertently share confidential details such as employee name, company name, job title, employee ID, email address, contact number, and home address. Target LLM: Grok
Strike AI LLM PII in User Requests Employee Record Disclosure - OpenAI		This strike involves crafting a user request that contains personally identifiable information (PII) related to employee records. The simulated request mimics real-world user behavior, where individuals might inadvertently share confidential details such as employee name, company name, job title, employee ID, email address, contact number, and home address. Target LLM: OpenAI
Strike AI LLM PII in User Requests Government Document Disclosure - Gemini		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: Gemini
Strike AI LLM PII in User Requests Government Document Disclosure - Grok		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: Grok
Strike AI LLM PII in User Requests Government Document Disclosure - OpenAI		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: OpenAI
Strike AI LLM PII in User Requests Protected Health Information (PHI) Disclosure - Gemini		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: Gemini
Strike AI LLM PII in User Requests Protected Health Information (PHI) Disclosure - Grok		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: Grok

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike AI LLM PII in User Requests Protected Health Information (PHI) Disclosure - OpenAI		This strike involves crafting a user request that contains personally identifiable information (PII) related to government records. The simulated request mimics real-world user behavior, where individuals might inadvertently share sensitive details such as citizen name, date of birth, SSN, passport number, home address, phone number and government employee ID. Target LLM: OpenAI
Strike AI LLM Prompt Injection Adaptive Attack Claude template - Gemini		This strike sends a AdaptiveAttack based jailbreak prompt type to the Gemini LLM. This attack sends refined-best-simple prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Gemini
Strike AI LLM Prompt Injection Adaptive Attack Claude template - Grok		This strike sends a AdaptiveAttack based jailbreak prompt type to the Grok LLM. This attack sends refined-best-simple prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Grok
Strike AI LLM Prompt Injection Adaptive Attack Claude template - OpenAI		This strike sends a AdaptiveAttack based jailbreak prompt type to the OpenAI LLM. This attack sends refined-best-simple prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: OpenAI
Strike AI LLM Prompt Injection Adaptive Attack ICL One Shot template - Gemini		This strike sends a AdaptiveAttack based jailbreak prompt type to the Gemini LLM. This attack sends icl-one-shot prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour Target LLM: Gemini
Strike AI LLM Prompt Injection Adaptive Attack ICL One Shot template - Grok		This strike sends a AdaptiveAttack based jailbreak prompt type to the Grok LLM. This attack sends icl-one-shot prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour Target LLM: Grok
Strike AI LLM Prompt Injection Adaptive Attack ICL One Shot template - OpenAI		This strike sends a AdaptiveAttack based jailbreak prompt type to the OpenAI LLM. This attack sends icl-one-shot prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour Target LLM: OpenAI

Name	References	Description
Strike AI LLM Prompt Injection Adaptive Attack Refined Best Simple template - Gemini		This strike sends a AdaptiveAttack based jailbreak prompt type to the Gemini LLM. This attack sends refined-best-simple prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Gemini
Strike AI LLM Prompt Injection Adaptive Attack Refined Best Simple template - Grok		This strike sends a AdaptiveAttack based jailbreak prompt type to the Grok LLM. This attack sends refined-best-simple prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Grok
Strike AI LLM Prompt Injection Adaptive Attack Refined Best Simple template - OpenAI		This strike sends a AdaptiveAttack based jailbreak prompt type to the OpenAI LLM. This attack sends refined-best-simple prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: OpenAI
Strike AI LLM Prompt Injection Adaptive Attack Refined Simple template - Gemini		This strike sends a AdaptiveAttack based jailbreak prompt type to the Gemini LLM. This attack sends refined-best prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Gemini
Strike AI LLM Prompt Injection Adaptive Attack Refined Simple template - Grok		This strike sends a AdaptiveAttack based jailbreak prompt type to the Grok LLM. This attack sends refined-best prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: Grok
Strike AI LLM Prompt Injection Adaptive Attack Refined Simple template - OpenAI		This strike sends a AdaptiveAttack based jailbreak prompt type to the OpenAI LLM. This attack sends refined-best prompt template which includes multiple malformed prompts with chaining adversarial suffix attached to the prompt. This attack can bypass keyword filters by tweaking the request prompt in every iteration in the prompt, effectively disguising jailbreak instructions to manipulate the LLM's behaviour. Target LLM: OpenAI
Strike AI LLM Prompt Injection P2SQL - Gemini		This strike sends a prompt to manipulate the Gemini LLM into generating a database-level CRUD (Create, Read, Update, Delete) operation. The request is designed to trigger the LLM into producing a SQL query that performs data manipulation tasks, such as creating new records, reading existing data, updating records, or deleting entries. The LLM's response includes a full SQL statement which, if executed, could result in unauthorized database changes or exposure of sensitive information. Target LLM: Gemini

Name	References	Description
Strike AI LLM Prompt Injection P2SQL - Grok		This strike sends a prompt to manipulate the Grok LLM into generating a database-level CRUD (Create, Read, Update, Delete) operation. The request is designed to trigger the LLM into producing a SQL query that performs data manipulation tasks, such as creating new records, reading existing data, updating records, or deleting entries. The LLM's response includes a full SQL statement which, if executed, could result in unauthorized database changes or exposure of sensitive information. Target LLM: Grok
Strike AI LLM Prompt Injection P2SQL - OpenAI		This strike sends a prompt to manipulate the OpenAI LLM into generating a database-level CRUD (Create, Read, Update, Delete) operation. The request is designed to trigger the LLM into producing a SQL query that performs data manipulation tasks, such as creating new records, reading existing data, updating records, or deleting entries. The LLM's response includes a full SQL statement which, if executed, could result in unauthorized database changes or exposure of sensitive information. Target LLM: OpenAI
Strike AI LLM ReNeLLM Alter Sentence Structure Scenario Code Completion - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and alters its sentence structure. The rewritten prompt is then sent to the Gemini LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Alter Sentence Structure Scenario Code Completion - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and alters its sentence structure. The rewritten prompt is then sent to the Grok LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Alter Sentence Structure Scenario Code Completion - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and alters its sentence structure. The rewritten prompt is then sent to the OpenAI LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM ReNeLLM Alter Sentence Structure Scenario Table Filling - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and alters its sentence structure. The rewritten prompt is then sent to the Gemini LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Alter Sentence Structure Scenario Table Filling - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and alters its sentence structure. The rewritten prompt is then sent to the Grok LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok

Name	References	Description
Strike AI LLM ReNeLLM Alter Sentence Structure Scenario Table Filling - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and alters its sentence structure. The rewritten prompt is then sent to the OpenAI LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM ReNeLLM Alter Sentence Structure Scenario Text Continuation - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and alters its sentence structure. The rewritten prompt is then sent to the Gemini LLM to generate a text continuation. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Alter Sentence Structure Scenario Text Continuation - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and alters its sentence structure. The rewritten prompt is then sent to the Grok LLM to generate a text continuation. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Alter Sentence Structure Scenario Text Continuation - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and alters its sentence structure. The rewritten prompt is then sent to the OpenAI LLM to generate a text continuation. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM ReNeLLM Insert Meaningless Characters Scenario Code Completion - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and inserts meaningless characters into the prompt. The rewritten prompt is then sent to the Gemini LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Insert Meaningless Characters Scenario Code Completion - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and inserts meaningless characters into the prompt. The rewritten prompt is then sent to the Grok LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Insert Meaningless Characters Scenario Code Completion - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and inserts meaningless characters into the prompt. The rewritten prompt is then sent to the OpenAI LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI

Name	References	Description
Strike AI LLM ReNeLLM Insert Meaningless Characters Scenario Text Continuation - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and inserts meaningless characters into the prompt. The rewritten prompt is then sent to the Gemini LLM to continue a text. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Insert Meaningless Characters Scenario Text Continuation - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and inserts meaningless characters into the prompt. The rewritten prompt is then sent to the Grok LLM to continue a text. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Insert Meaningless Characters Scenario Text Continuation - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and inserts meaningless characters into the prompt. The rewritten prompt is then sent to the OpenAI LLM to continue a text. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM ReNeLLM Insert Meaningless Characters Scenario Table Filling - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and inserts meaningless characters into the prompt. The rewritten prompt is then sent to the Gemini LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Insert Meaningless Characters Scenario Table Filling - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and inserts meaningless characters into the prompt. The rewritten prompt is then sent to the Grok LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Insert Meaningless Characters Scenario Table Filling - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and inserts meaningless characters into the prompt. The rewritten prompt is then sent to the OpenAI LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM ReNeLLM Misspell Sensitive Words Scenario Code Completion - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and misspells sensitive words in the prompt. The rewritten prompt is then sent to the Gemini LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini

Name	References	Description
Strike AI LLM ReNeLLM Misspell Sensitive Words Scenario Code Completion - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and misspells sensitive words in the prompt. The rewritten prompt is then sent to the Grok LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Misspell Sensitive Words Scenario Code Completion - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and misspells sensitive words in the prompt. The rewritten prompt is then sent to the OpenAI LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM ReNeLLM Misspell Sensitive Words Scenario Table Filling - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and misspells sensitive words in the prompt. The rewritten prompt is then sent to the Gemini LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Misspell Sensitive Words Scenario Table Filling - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and misspells sensitive words in the prompt. The rewritten prompt is then sent to the Grok LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Misspell Sensitive Words Scenario Table Filling - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and misspells sensitive words in the prompt. The rewritten prompt is then sent to the OpenAI LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM ReNeLLM Misspell Sensitive Words Scenario Text Continuation - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and misspells sensitive words in the prompt. The rewritten prompt is then sent to the Gemini LLM to continue a text. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Misspell Sensitive Words Scenario Text Continuation - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and misspells sensitive words in the prompt. The rewritten prompt is then sent to the Grok LLM to continue a text. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Misspell Sensitive Words Scenario Text Continuation - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and misspells sensitive words in the prompt. The rewritten prompt is then sent to the OpenAI LLM to continue a text. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI

Name	References	Description
Strike AI LLM ReNeLLM Paraphrasing Scenario Code Completion - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and paraphrases it with fewer words. The rewritten prompt is then sent to the Gemini LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Paraphrasing Scenario Code Completion - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and paraphrases it with fewer words. The rewritten prompt is then sent to the Grok LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Paraphrasing Scenario Code Completion - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and paraphrases it with fewer words. The rewritten prompt is then sent to the OpenAI LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM ReNeLLM Paraphrasing Scenario Table Filling - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and paraphrases it with fewer words. The rewritten prompt is then sent to the Gemini LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Paraphrasing Scenario Table Filling - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and paraphrases it with fewer words. The rewritten prompt is then sent to the Grok LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Paraphrasing Scenario Table Filling - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and paraphrases it with fewer words. The rewritten prompt is then sent to the OpenAI LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM ReNeLLM Paraphrasing Scenario Text Continuation - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and paraphrases it with fewer words. The altered prompt is then sent to the Gemini LLM to generate a text continuation. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini

Name	References	Description
Strike AI LLM ReNeLLM Paraphrasing Scenario Text Continuation - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and paraphrases it with fewer words. The altered prompt is then sent to the Grok LLM to generate a text continuation. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Paraphrasing Scenario Text Continuation - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and paraphrases it with fewer words. The altered prompt is then sent to the OpenAI LLM to generate a text continuation. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM ReNeLLM Partial Translation Scenario Code Completion - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and partially translates it. The rewritten prompt is then sent to the Gemini LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Partial Translation Scenario Code Completion - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and partially translates it. The rewritten prompt is then sent to the Grok LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Partial Translation Scenario Code Completion - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and partially translates it. The rewritten prompt is then sent to the OpenAI LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM ReNeLLM Partial Translation Scenario Table Filling - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and partially translates it. The rewritten prompt is then sent to the Gemini LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Partial Translation Scenario Table Filling - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and partially translates it. The rewritten prompt is then sent to the Grok LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Partial Translation Scenario Table Filling - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and partially translates it. The rewritten prompt is then sent to the OpenAI LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI

Name	References	Description
Strike AI LLM ReNeLLM Partial Translation Scenario Text Continuation - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and partially translate it. The rewritten prompt is then sent to the Gemini LLM to generate a text continuation. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Partial Translation Scenario Text Continuation - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and partially translate it. The rewritten prompt is then sent to the Grok LLM to generate a text continuation. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Partial Translation Scenario Text Continuation - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and partially translate it. The rewritten prompt is then sent to the OpenAI LLM to generate a text continuation. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM ReNeLLM Style Change Scenario Code Completion - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and changes its expression style. The rewritten prompt is then sent to the Gemini LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Style Change Scenario Code Completion - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and changes its expression style. The rewritten prompt is then sent to the Grok LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Style Change Scenario Code Completion - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and changes its expression style. The rewritten prompt is then sent to the OpenAI LLM to generate a code completion. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM ReNeLLM Style Change Scenario Table Filling - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and changes its expression style. The rewritten prompt is then sent to the Gemini LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Style Change Scenario Table Filling - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and changes its expression style. The rewritten prompt is then sent to the Grok LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok

Name	References	Description
Strike AI LLM ReNeLLM Style Change Scenario Table Filling - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and changes its expression style. The rewritten prompt is then sent to the OpenAI LLM to fill a table. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM ReNeLLM Style Change Scenario Text Continuation - Gemini		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Gemini LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and changes its expression style. The rewritten prompt is then sent to the Gemini LLM to generate a text continuation. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Gemini
Strike AI LLM ReNeLLM Style Change Scenario Text Continuation - Grok		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the Grok LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and changes its expression style. The rewritten prompt is then sent to the Grok LLM to generate a text continuation. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: Grok
Strike AI LLM ReNeLLM Style Change Scenario Text Continuation - OpenAI		This strike sends a Prompt Rewriting and Scenario Nesting (ReNe)-based prompt to the OpenAI LLM. It randomly selects a jailbreak prompt from the ReNeLLM dataset and changes its expression style. The rewritten prompt is then sent to the OpenAI LLM to generate a text continuation. The attack is designed to bypass the LLM's safety mechanisms and generate malicious responses. Target LLM: OpenAI
Strike AI LLM Prompt Injection SMILES-Prompting Substance - Gemini		This strike leverages SMILES (Simplified Molecular-Input Line-Entry System) structural notation to reference chemical substances instead of their conventional names to bypass LLM guardrails and keyword filters, thus providing jailbreak instructions to manipulate its behaviour and in turn, generate synthesis instructions for harmful and/or banned substances. Target LLM: Gemini
Strike AI LLM Prompt Injection SMILES-Prompting Substance - Grok		This strike leverages SMILES (Simplified Molecular-Input Line-Entry System) structural notation to reference chemical substances instead of their conventional names to bypass LLM guardrails and keyword filters, thus providing jailbreak instructions to manipulate its behaviour and in turn, generate synthesis instructions for harmful and/or banned substances. Target LLM: Grok
Strike AI LLM Prompt Injection SMILES-Prompting Substance - OpenAI		This strike leverages SMILES (Simplified Molecular-Input Line-Entry System) structural notation to reference chemical substances instead of their conventional names to bypass LLM guardrails and keyword filters, thus providing jailbreak instructions to manipulate its behaviour and in turn, generate synthesis instructions for harmful and/or banned substances. Target LLM: OpenAI

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Adobe Acrobat JBIG2 Stream Indexing Overflow (SMTP Quoted Printable)	CWE: 119 CVE: 2009-0658 BID: 33751	This strike exploits a stream indexing vulnerability first discovered in Adobe Acrobat when parsing PDF files with malformed JBIG2 streams. This vulnerability is believed to also affect other PDF implementations.
Strike Adobe Acrobat Reader customDictionaryOpen Memory Corruption (SMTP Base64)	CWE: 399 CVE: 2009-1493 BID: 34740	This strike exploits a flaw in Adobe's PDF reader that can result in the execution of arbitrary code.
Strike Adobe Acrobat Reader customDictionaryOpen Memory Corruption (SMTP Quoted Printable)	CWE: 399 CVE: 2009-1493 BID: 34740	This strike exploits a flaw in Adobe's PDF reader that can result in the execution of arbitrary code.
Strike Adobe Acrobat Reader getIcon Memory Corruption (SMTP Base64)	BID: 34169 CWE: 20 CVE: 2009-0927	This strike exploits a flaw in Adobe's PDF reader that can result in the execution of arbitrary code.
Strike Adobe Acrobat Reader getIcon Memory Corruption (SMTP Quoted Printable)	BID: 34169 CWE: 20 CVE: 2009-0927	This strike exploits a flaw in Adobe's PDF reader that can result in the execution of arbitrary code.
Strike Adobe Illustrator CS4 .eps Buffer Overflow (SMTP Quoted Printable)	CWE: 119 CVE: 2009-4195 BID: 37192	This strike exploits a vulnerability in the way Adobe Illustrator parses Encapsulated Postscript files containing an overly long strings in a DSC comment, causing a buffer overflow and resulting in possible code execution.
Strike Apple OS X QuickDraw GetSrcBits32ARGB Memory Corruption Denial of Service (SMTP)	BID: 22207 CVE: 2007-0462	This strike exploits a denial of service condition in Apple's Mac OS X when opening a malformed PICT file.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Flip4Mac Memory Corruption (SMTP)	BID: 22286 CVE: 2007-0466	This strike exploits a memory corruption flaw in Telestream Flip4Mac when handling WMF files.
Strike GDIPPlus JPEG Processing Buffer Overrun - SMTP Message	BID: 11173 CVE: 2004-0200	This strike exploits a vulnerability in the processing of JPEG images in multiple Microsoft products based on the GDIPPlus image library. This strike simulates attaching a JPEG to an SMTP message.
Strike Internet Explorer EMF File Rendering Denial of Service (SMTP)	CWE: 399 CVE: 2005-0803 BID: 12834	This strike exploits a denial of service flaw in Microsoft Windows. This flaw is triggered through a malformed Windows EMF Metafile. This strike simulates downloading an EMF file via SMTP.
Strike Internet Explorer WMF File Rendering Denial of Service (SMTP)	CVE: 2005-2124 BID: 15356	This strike exploits a denial of service flaw in Microsoft Windows. This flaw is triggered through a malformed Windows WMF Metafile. This strike simulates downloading an WMF file via SMTP.
Strike Mac OS X DMG UFS ffs_mountfs() Integer Overflow (SMTP)	BID: 21993 CWE: 189 CVE: 2007-0229	This strike transfers a malicious disk image (DMG) file to a Mac OS X target.
Strike Mac OS X Finder DMG Volume Name Memory Corruption (SMTP)	BID: 21980 CWE: 119 CVE: 2007-0197	This transfers a malicious disk image (DMG) file to a Mac OS X target.
Strike Malformed AU File Divide-by-Zero Denial of Service (SMTP)		This strike exploits a denial of service flaw in programs that handle .au files without detecting a divide-by-zero condition
Strike Microsoft Color Management ColorMatchToTarget W (SMTP Quoted Printable)	BID: 30594 CWE: 119 CVE: 2008-2245	This strike exploits a memory corruption vulnerability in the Microsoft Windows Color Management System when handling EMF files with a crafted EMR_COLORMATCHTOTARGETW record.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Excel BIFF Record Parsing Vulnerability (SMTP Base64)	BID: 31705 CWE: 399 CVE: 2008-3471	This strike exploits a vulnerability in Microsoft Excel when parsing a file containing crafted BIFF records.
Strike Microsoft Excel BIFF Record Parsing Vulnerability (SMTP Quoted Printable)	BID: 31705 CWE: 399 CVE: 2008-3471	This strike exploits a vulnerability in Microsoft Excel when parsing a file containing crafted BIFF records.
Strike Microsoft Excel Embedded Object Validation Vulnerability (SMTP Base64)	BID: 31702 CWE: 399 CVE: 2008-3477	This strike exploits a vulnerability in Microsoft Excel when parsing a file containing an embedded object.
Strike Microsoft Excel Embedded Object Validation Vulnerability (SMTP Quoted Printable)	BID: 31702 CWE: 399 CVE: 2008-3477	This strike exploits a vulnerability in Microsoft Excel when parsing a file containing an embedded object.
Strike Microsoft Excel NULL Pointer DoS (A) (SMTP)	BID: 22717 CVE: 2007-1239	This strike exploits a denial of service flaw in Microsoft Excel using a corrupted XLS document.
Strike Microsoft Excel NULL Pointer DoS (B) (SMTP)	BID: 22717 CVE: 2007-1239	This strike exploits a denial of service flaw in Microsoft Excel using a corrupted XLS document.
Strike Microsoft Excel Obj Record Invalid Subtype Vulnerability (SMTP Base64)	BID: 32621 CWE: 399 CVE: 2008-4264	This strike exploits a vulnerability in Microsoft Excel when parsing a file containing an embedded object with an invalid subtype record.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Excel Obj Record Invalid Subtype Vulnerability (SMTP Quoted Printable)	BID: 32621 CWE: 399 CVE: 2008-4264	This strike exploits a vulnerability in Microsoft Excel when parsing a file containing an embedded object with an invalid subtype record.
Strike Microsoft Excel REPT() Formula Parsing Vulnerability (SMTP Base64)	BID: 31706 CWE: 189 CVE: 2008-4019	This strike exploits a vulnerability in Microsoft Excel when evaluating a REPT() formula with a long number_times parameter.
Strike Microsoft Excel REPT() Formula Parsing Vulnerability (SMTP Quoted Printable)	BID: 31706 CWE: 189 CVE: 2008-4019	This strike exploits a vulnerability in Microsoft Excel when evaluating a REPT() formula with a long number_times parameter.
Strike Microsoft Office Memory Corruption (PowerPoint) (SMTP Base64)	BID: 28146 CWE: 94 CVE: 2008-0118	This strike exploits a memory corruption vulnerability in the Microsoft Office XP PowerPoint component.
Strike Microsoft Office Memory Corruption (PowerPoint) (SMTP Quoted Printable)	BID: 28146 CWE: 94 CVE: 2008-0118	This strike exploits a memory corruption vulnerability in the Microsoft Office XP PowerPoint component.
Strike Microsoft Office Smart Tag WordCount Memory Corruption (SMTP Base64)	BID: 30124 CWE: 399 CVE: 2008-2244	This strike exploits a memory corruption vulnerability in Microsoft Office that is triggered when a Smart Tag structure containing an invalid WordCount value.
Strike Microsoft Office Smart Tag WordCount Memory Corruption (SMTP Quoted Printable)	BID: 30124 CWE: 399 CVE: 2008-2244	This strike exploits a memory corruption vulnerability in Microsoft Office that is triggered when a Smart Tag structure containing an invalid WordCount value.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Office Text Converter Integer Underflow Code Execution (SMTP Direct Quoted Printable)	CVE: 2009-0087	This strike exploits an integer underflow code execution vulnerability in Microsoft Office's text convertor.
Strike Microsoft PowerPoint Master Style Integer Overflow (SMTP Base64)	BID: 30579 CWE: 399 CVE: 2008-1455	This strike exploits a memory corruption vulnerability in Microsoft PowerPoint when opening a file with a malformed Master Style attribute.
Strike Microsoft PowerPoint Master Style Integer Overflow (SMTP Quoted Printable)	BID: 30579 CWE: 399 CVE: 2008-1455	This strike exploits a memory corruption vulnerability in Microsoft PowerPoint when opening a file with a malformed Master Style attribute.
Strike Microsoft PowerPoint TextHeaderAtom Freed Memory Heap Corruption (SMTP Base64)	BID: 34351 CWE: 94 CVE: 2009-0556	This strike exploits a heap memory corruption vulnerability in Microsoft Office's PowerPoint.
Strike Microsoft PowerPoint TextHeaderAtom Freed Memory Heap Corruption (SMTP Quoted Printable)	BID: 34351 CWE: 94 CVE: 2009-0556	This strike exploits a heap memory corruption vulnerability in Microsoft Office's PowerPoint.
Strike Microsoft PowerPoint Viewer 2003 MSODRAWING Property Heap Overflow (SMTP Base64)	BID: 30554 CWE: 399 CVE: 2008-0121	This strike exploits a memory corruption vulnerability in Microsoft PowerPoint Viewer when processing a file with a malformed MSODRAWING Property Table.
Strike Microsoft PowerPoint Viewer 2003 MSODRAWING Property Heap Overflow (SMTP Quoted Printable)	BID: 30554 CWE: 399 CVE: 2008-0121	This strike exploits a memory corruption vulnerability in Microsoft PowerPoint Viewer when processing a file with a malformed MSODRAWING Property Table.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft PowerPoint Viewer 2003 Picture Array Index (SMTP Base64)	BID: 30552 CWE: 399 CVE: 2008-0120	This strike exploits an out-of-bounds array index vulnerability in Microsoft PowerPoint Viewer 2003 when reading malformed PowerPoint files.
Strike Microsoft PowerPoint Viewer 2003 Picture Array Index (SMTP Quoted Printable)	BID: 30552 CWE: 399 CVE: 2008-0120	This strike exploits an out-of-bounds array index vulnerability in Microsoft PowerPoint Viewer 2003 when reading malformed PowerPoint files.
Strike Microsoft Windows Color Management Module ICC Profile Buffer Overflow (SMTP)	CVE: 2005-1219 BID: 14214	Microsoft Windows has a buffer overflow vulnerability in the processing of malformed image files. This strike simulates downloading a JPEG via SMTP.
Strike Microsoft Windows EMF Polylines (SMTP Quoted Printable)	BID: 34012 CWE: 20 CVE: 2009-0081	This strike exploits a vulnerability in Microsoft Windows when parsing an EMF file with crafted EMR_POLYLINE data.
Strike Microsoft Windows GDI Stack Overflow (SMTP Base64)	BID: 28570 CWE: 119 CVE: 2008-1087	This strike sends a file that exploits a stack overflow flaw in GDI, a core component of the Microsoft Windows Graphical User Interface
Strike Microsoft Windows GDI Stack Overflow (SMTP Quoted Printable)	BID: 28570 CWE: 119 CVE: 2008-1087	This strike sends a file that exploits a stack overflow flaw in GDI, a core component of the Microsoft Windows Graphical User Interface
Strike Microsoft Windows LoadImage API Overflow (SMTP)	BID: 12095 CVE: 2004-1049	This strike exploits a flaw in the parsing of images via LoadImage on Microsoft Windows. This strike simulates sending a malicious .ani animated cursor in a SMTP message.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Word 2000 Malformed Function Code Execution (SMTP)	CVE: 2007-0515 BID: 22225	This strike exploits a code execution flaw in Microsoft Word 2000 that is triggered by a malformed function definition.
Strike Microsoft Word Memory Corruption Vulnerability (SMTP) (Arbitrary Free Base64)	CWE: 94 CVE: 2008-4024	This strike exploits a vulnerability in MS Word that allows a malicious document to run 'free()' on an arbitrary address.
Strike Microsoft Word Memory Corruption Vulnerability (SMTP) (Arbitrary Free Quoted Printable)	CWE: 94 CVE: 2008-4024	This strike exploits a vulnerability in MS Word that allows a malicious document to run 'free()' on an arbitrary address.
Strike Microsoft Word Memory Corruption Vulnerability (SMTP) (Array Index Base64)	CWE: 399 CVE: 2008-4026	This strike exploits a vulnerability in MS Word that uses an unchecked offset into an array.
Strike Microsoft Word Memory Corruption Vulnerability (SMTP) (Array Index Quoted Printable)	CWE: 399 CVE: 2008-4026	This strike exploits a vulnerability in MS Word that uses an unchecked offset into an array.
Strike Microsoft Word RTF Object Parsing Vulnerability (SMTP Quoted Printable)	CWE: 399 CVE: 2008-4027	This strike exploits a vulnerability in MS Word caused by an RTF file with invalid '\do' directives.
Strike Microsoft Word RTF Object Parsing Vulnerability (dpcallout) (SMTP Quoted Printable)	CWE: 119 CVE: 2008-4028	This strike exploits a vulnerability in MS Word caused by an RTF file with invalid '\dpcallout' directives.
Strike Microsoft Word RTF Object Parsing Vulnerability (dpendgroup) (SMTP Quoted Printable)	CWE: 399 CVE: 2008-4030	This strike exploits a vulnerability in MS Word caused by an RTF file with invalid '\dpendgroup' directives.
Strike Microsoft Word RTF Object Parsing Vulnerability (dpolycount) (SMTP Quoted Printable)	CWE: 119 CVE: 2008-4025	This strike exploits a vulnerability in MS Word caused by an RTF file with an invalid '\dpolycount' directive.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Microsoft Word RTF Object Parsing Vulnerability (stylesheet) (SMTP Quoted Printable)	CWE: 399 CVE: 2008-4031	This strike exploits a vulnerability in MS Word caused by an RTF file with invalid '\stylesheet' directives.
Strike Microsoft Word Table Property Stack Overflow (SMTP Base64)	CWE: 119 CVE: 2008-4837	This strike exploits a vulnerability in MS Word caused when processing an invalid table property.
Strike Microsoft Word Table Property Stack Overflow (SMTP Quoted Printable)	CWE: 119 CVE: 2008-4837	This strike exploits a vulnerability in MS Word caused when processing an invalid table property.
Strike Microsoft WordPad Embedded COM Code Execution (AddressBook) (SMTP)		This strike exploits a flaw in Microsoft WordPad that can be used to execute arbitrary code. This particular strike embeds the OutlookExpress.AddressBook COM control into the OLE section of a WordPad RTF document.
Strike Microsoft WordPad Embedded COM Code Execution (InstallEngine) (SMTP)		This strike exploits a flaw in Microsoft WordPad that can be used to execute arbitrary code. This particular strike embeds the InstallEngine COM control into the OLE section of a WordPad RTF document.
Strike Microsoft WordPad Embedded COM Code Execution (Sysmon.3) (SMTP)		This strike exploits a flaw in Microsoft WordPad that can be used to execute arbitrary code. This particular strike embeds the Sysmon.3 COM control into the OLE section of a WordPad RTF document and defines a set of corrupt OLE properties that will cause a crash on load.
Strike Microsoft Works RTF File Conversion Buffer Overflow (SMTP Base64)	BID: 27659 CWE: 119 CVE: 2008-0108	This strike exploits a buffer overflow in the Microsoft Office and Microsoft Works file converter. A buffer overflow can be triggered when a corrupted Microsoft Works file is converted to the Rich Text Format (RTF).
Strike Microsoft Works RTF File Conversion Buffer Overflow (SMTP Quoted Printable)	BID: 27659 CWE: 119 CVE: 2008-0108	This strike exploits a buffer overflow in the Microsoft Office and Microsoft Works file converter. A buffer overflow can be triggered when a corrupted Microsoft Works file is converted to the Rich Text Format (RTF).

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike VLC Ogg Vorbis Comment Header Format String (SMTP)	BID: 24555  CVE: 2007-3316	This strike exploits a format string vulnerability in VLC when decoding Ogg Vorbis files. This strike simulates sending a malicious file via SMTP.
Strike Windows Explorer.exe AVI Right Click Denial of Service (SMTP)	CVE: 2007-0562	This strike exploits a denial of service condition in Microsoft Windows explorer.exe when right-clicking on a malformed AVI file.
Strike Windows GDI Malformed Image Denial of Service (SMTP)	BID: 25302  CWE: 189  CVE: 2007-3034	This strike exploits a denial-of-service vulnerability in Windows when handling malformed WMF files
Strike Windows OLE32.dll Word Document Handling Denial of Service (SMTP)	CWE: 119  CVE: 2007-1347  BID: 22847	This strike exploits a denial of service condition in Microsoft Windows OLE32.dll when parsing a malicious Word document.
Strike Windows Object Packager Dialogue Spoofing (SMTP)	CWE: 94  CVE: 2006-4692  BID: 20318	This strike exploits a dialogue spoofing flaw in the Windows Object Packager. This flaw allows an attacker to embed a malicious object within a RTF or Microsoft Office document that appears to be a safe file type.
Strike Windows Shortcut Font Name Overflow (SMTP)	CVE: 2005-2118  CVE: 2005-0550  BID: 15070  BID: 13115	This strike exploits two different vulnerabilities in the Windows operating system. The first flaw triggers a stack overflow in the CSrss process when a malformed shortcut is opened. The second flaw triggers a stack overflow in Windows Explorer when the properties of a malformed shortcut file are viewed.
Strike libpng png_handle_sBIT() Local Overflow (SMTP)	BID: 10857  BID: 15495  CVE: 2004-0597	This strike exploits a vulnerability in the processing of PNG images by libpng. This strike simulates sending a PNG via SMTP.

<b>Name</b>	<b>References</b>	<b>Description</b>
Strike Brute Force Attack		Brute-force attacks are techniques that an attacker may employ in order to gain access to accounts. Such techniques involve password spraying and credential stuffing where the attacker is repeatedly trying to find correct credential pairs using small lists of common or known passwords against a list of potential user accounts
Strike URL Filtering	CWE: 790	This strike utilizes special URLs in order to exploit different vulnerabilities.
Strike URL Filtering - Separate Host and Path	CWE: 790	This strike utilizes special URLs in order to exploit different vulnerabilities. When using in a customized attack, make sure to explicitly configure the Host parameter to use the Host column of the same Playlist file as the Path parameter. The Host parameter can be modified from the Attack's Advanced Settings > Connections > Hostname.
Strike Vector HTTP POST	CWE: 89 CWE: 79	Template strike used with a configurable HTTP POST request which can simulate SQL Injection attacks targeting web applications by inserting SQL statements into HTTP request data (such as forms, HTTP headers, URL parameters or message body). These attacks take advantage of unsanitized data to subvert the query executed on the database by inserting SQL statement into HTTP request. This attack contains a collection of SQL Injection payloads coming from multiple public sources and private resources. Cross-Site Scripting (XSS) is a type of computer security vulnerability found in websites that enables attackers to inject scripts into web pages viewed by other users. When these scripts are viewed and executed by other users, they can steal credentials, sensitive data, or modify values or settings on the target website. Reflected XSS (known also as non-persistent XSS) is taking place when the script is not stored on the Web Application side. Typically, the XSS code is spread by sharing a link which is referring a vulnerable web page. The link itself includes the malicious code to execute in web browsers.
Strike SQL Injection and XSS Vector	CWE: 89 CWE: 79	SQL Injection attacks target web applications by inserting SQL statements into HTTP request data (such as forms, HTTP headers or URL parameters). These attacks take advantage of unsanitized data to subvert the query executed on the database by inserting SQL statement into HTTP request. Cross-Site Scripting (XSS) is a type of computer security vulnerability found in websites that enables attackers to inject scripts into web pages viewed by other users. When these scripts are viewed and executed by other users, they can steal credentials, sensitive data, or modify values or settings on the target website. Reflected XSS (known also as non-persistent XSS) is taking place when the script is not stored on the Web Application side. Typically, the XSS code is spread by sharing a link which is referring a vulnerable web page. The link itself includes the malicious code to execute in web browsers. This attack contains a collection of SQL Injection payloads coming from multiple public sources and private resources.

Name	References	Description
Strike Vector Webshell	CWE: 89 CWE: 79	Webshells are malicious scripts that facilitate remote administration once installed on a web server, enabling the execution of malicious commands for a wide range of scenarios: exfiltrating and harvesting information, uploading malware, modifying or adding files. Webshells represent a backdoor into the targeted system, enabling remote attackers to access the host and even move laterally. This strike can be used to simulate a webshell attack by uploading a malicious file on the server.
Strike Vector Webshell Payload	CWE: 89 CWE: 79	Webshells are malicious scripts that facilitate remote administration once installed on a web server, enabling the execution of malicious commands for a wide range of scenarios: exfiltrating and harvesting information, uploading malware, modifying or adding files. Webshells represent a backdoor into the targeted system, enabling remote attackers to access the host and even move laterally. This strike can be used to simulate a webshell attack by uploading a malicious file on the server.

## All Malware Samples (6755)

Name	Description
Strike APTC60_6669d4a8	This strike sends a malware sample known as APTC60. APTC-60 is a threat group that has recently been associated with cyber attacks against Japanese organizations. This malware is part of an attack chain that consists of a phishing email that led to the download of a VHDX file that executes a PE binary and generates a downloader. This downloader then further downloads a backdoor that establishes communication and persistence on the target. The MD5 hash of this APTC60 sample is 6669d4a8a2c9319e1faa80123e6f0d5a.
Strike APTC60_78b4d05a	This strike sends a malware sample known as APTC60. APTC-60 is a threat group that has recently been associated with cyber attacks against Japanese organizations. This malware is part of an attack chain that consists of a phishing email that led to the download of a VHDX file that executes a PE binary and generates a downloader. This downloader then further downloads a backdoor that establishes communication and persistence on the target. The MD5 hash of this APTC60 sample is 78b4d05a7d81b1cd96f1844ce4b201b3.
Strike APTC60_d6a2c8d7	This strike sends a malware sample known as APTC60. APTC-60 is a threat group that has recently been associated with cyber attacks against Japanese organizations. This malware is part of an attack chain that consists of a phishing email that led to the download of a VHDX file that executes a PE binary and generates a downloader. This downloader then further downloads a backdoor that establishes communication and persistence on the target. The MD5 hash of this APTC60 sample is d6a2c8d7a5546de3b5eaa1c92865d001.
Strike AceCryptor_0b7af822	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 0b7af822f9c85668d446d0d6d26903cb.

<b>Name</b>	<b>Description</b>
Strike AceCryptor_10a08ec8	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 10a08ec8fd17e9b73e62568d5ab8a9b3.
Strike AceCryptor_26ba1146	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 26ba1146f36c3703f94ce7e5602cd3da.
Strike AceCryptor_2cb2a55a	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 2cb2a55af83803b57caa53a21dec20b0.
Strike AceCryptor_454dc3fc	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 454dc3fc0921ce440ec8780b8e5992fb.
Strike AceCryptor_47bf6bfc	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 47bf6bfc52defe05b87d0e04e3d92c45.
Strike AceCryptor_49800f6e	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 49800f6e90bf6019da4a13639032642f.
Strike AceCryptor_59eec747	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 59eec747286f1e89ce96fef39f9de3e5.
Strike AceCryptor_5b2f54fb	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 5b2f54fbca30e9a282f3d8b461e03a17.

<b>Name</b>	<b>Description</b>
Strike AceCryptor_5cb1682f	This strike sends a polymorphic malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this AceCryptor sample is 5cb1682f8281d6e72463f74336ebe258.
Strike AceCryptor_5ea12c54	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 5ea12c54a54b31b61629188545e432cc.
Strike AceCryptor_634b1183	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 634b1183d01be4d8ffb806a4827ed879.
Strike AceCryptor_6c90215b	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 6c90215b8a560ecb2f5f2430b1f2e016.
Strike AceCryptor_6e243f38	This strike sends a polymorphic malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this AceCryptor sample is 6e243f384f7c494c284fe4113d7d8c8a.
Strike AceCryptor_79871e44	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 79871e44f79f36393c2c9beb8e366125.
Strike AceCryptor_7abe5257	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 7abe5257dbe779a37c1715a3d8e2bd9d.

<b>Name</b>	<b>Description</b>
Strike AceCryptor_7e1d6a44	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 7e1d6a44d1cf118a3752e17972a4d69c.
Strike AceCryptor_804bf188	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 804bf188fd3fd4d9afdbc1ff0d020cda.
Strike AceCryptor_8741c48f	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 8741c48f70c18d6337558bbd676f5a0d.
Strike AceCryptor_8b9b33a5	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 8b9b33a5183fde571a18583844432eb3.
Strike AceCryptor_8dbdef61	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 8dbdef6108e6b202ecc0570c9e96d76b.
Strike AceCryptor_9d5512a5	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is 9d5512a57dfdc484cb7ee15668ab6e22.
Strike AceCryptor_b95b574d	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is b95b574d4233b2cbc00ad5bc0e1721e7.
Strike AceCryptor_cc492729	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is cc492729431765a9bc9cbf54625a6dac.

<b>Name</b>	<b>Description</b>
Strike AceCryptor_e320bb75	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is e320bb753ba6fb13ea7ef15e7efc315e.
Strike AceCryptor_e9cb900e	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is e9cb900e57154d6469dae21c82a1753b.
Strike AceCryptor_f18129ea	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is f18129ea81b3b5690cf1300397db51e.
Strike AceCryptor_f22089ec	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is f22089ecc61519c668e9f7ae4f0fe372.
Strike AceCryptor_f9027bda	This strike sends a polymorphic malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The binary has the checksum removed in the PE file format. The MD5 hash of this AceCryptor sample is f9027bdaa0eb5a4017a16f6e2d50f5f1.
Strike AceCryptor_fa0ce1b2	This strike sends a polymorphic malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this AceCryptor sample is fa0ce1b21f49a9bcb382759a5052ec1c.
Strike AceCryptor_fcf22de7	This strike sends a polymorphic malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The binary has random bytes appended at the end of the file. The MD5 hash of this AceCryptor sample is fcf22de7f4cb40a21878236aecb0687c.

<b>Name</b>	<b>Description</b>
Strike AceCryptor_fe1cfddb	This strike sends a malware sample known as AceCryptor. AceCryptor is a cryptor-as-a-service that is used to pack numerous malware families. These samples are part of an email campaign that delivered the cryptor as a malicious attachment. It contains an iso file or archive that once executed unpacks and launches the Rescoms , also known as Remcos, RAT. The MD5 hash of this AceCryptor sample is fe1cfddb7b44cec0b5c37769934a2ee9.
Strike AcidRain_ecbe1b1e	This strike sends a malware sample known as AcidRain. AcidRain is a wiper malware associated with the Russian invasion of Ukraine, and was used in 2022 in an attack against Viasat modems. It is a MIPS ELF binary that performs a wipe of the target filesystem. The malware also shares some common linked libraries with the VPNFilter plugin , 'dstr', which was meant to wipe devices. The MD5 hash of this AcidRain sample is ecbe1b1e30a1f4bfffaf1d374014c877f.
Strike Adrozek_022fd996	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 022fd9966a974597ef3ea8a2053eebab.
Strike Adrozek_12168815	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 12168815ad176df39aac31d8680e8e63.
Strike Adrozek_195cbbfd	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 195cbbfd4bb76b0fe346ad80df06f627.
Strike Adrozek_2ad72cab	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 2ad72cab2e2307bc31d2796f9b860f9f.
Strike Adrozek_37c8cd08	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 37c8cd0861e71380adf860424819b9f2.
Strike Adrozek_3ff3ab8e	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 3ff3ab8ea667738e005cb419c51d1960.
Strike Adrozek_4c0b0223	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 4c0b0223e8703e5347038ca240c8f703.
Strike Adrozek_512870c5	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 512870c58ca92bf9cf31969e6ff95233.
Strike Adrozek_55499c0c	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 55499c0c9d2df98f821ed55071f5bc1c.

<b>Name</b>	<b>Description</b>
Strike Adrozek_55dd45f4	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 55dd45f49c6f87bc0e838313e29ed47f.
Strike Adrozek_68fc74f9	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 68fc74f99d0665401261f7cb9d5967db.
Strike Adrozek_6ab15660	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 6ab15660f883d6c313a84f3092c2af7c.
Strike Adrozek_76dc151b	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 76dc151b8ef17e2b51180919e40e3d7f.
Strike Adrozek_807592e6	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 807592e6eb531ffeb53a27c0f62b71b7.
Strike Adrozek_85120da5	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 85120da5492577b6e462bcaf567302c5.
Strike Adrozek_85172625	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 8517262559ecf71f29621ba6a2fa79e9.
Strike Adrozek_88bcf085	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is 88bcf0852d8b458e5629596ef0c7871b.
Strike Adrozek_cc3ab50b	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is cc3ab50be1cfacb7860ee1f3776e57e0.
Strike Adrozek_ce83b6ce	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is ce83b6ce2230e9069de9e65310793aa6.
Strike Adrozek_dcb287af	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is dc当地b287aff31159ff8e4fc6d8b3343036.
Strike Adrozek_f16f2431	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is f16f24310f498026a447286847b83c54.

<b>Name</b>	<b>Description</b>
Strike Adrozek_fb187560	This strike sends a malware sample known as Adrozek. Adrozek hooks into web browsers to inject ads on webpages and steals login credentials when users visit the webpage. The MD5 hash of this Adrozek sample is fb1875607626cab63dfd07273c45fc7f.
Strike Allakore_058bde7b	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 058bde7b3385b70d59120b24390377af.
Strike Allakore_09096930	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 09096930751d28d388d3e0de003bcb7b.
Strike Allakore_12dbbfcc	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 12dbbfcccd463ec884f788abd5933f8aa.
Strike Allakore_237a12a9	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 237a12a9d67614edd079c02f0f24ed45.
Strike Allakore_29a9d202	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 29a9d202ba2d46047edba9539abba0cd.
Strike Allakore_2f0b96c3	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 2f0b96c3262108012dcf9a940ae461da.
Strike Allakore_32d491d6	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 32d491d6b036c6349c4d2c3bf44011d8.
Strike Allakore_35932f58	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 35932f5856dbf8ba51e048b3b2bb2d7b.

<b>Name</b>	<b>Description</b>
Strike Allakore_3bed8895	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 3bed8895828ba27761b62e9c4ebcc2db.
Strike Allakore_40291ec2	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 40291ec2bd7f23aa76435d5d14f96758.
Strike Allakore_42300099	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 42300099a726353abfdbfd5773de83.
Strike Allakore_47ead282	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 47ead282cd7c6a667d9b4cc9b0c6935e.
Strike Allakore_59401f25	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 59401f25ac88f1c1fe0a5981dc29ea57.
Strike Allakore_59c6ae6b	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 59c6ae6bbe3d048d267d4900c9585828.
Strike Allakore_733f33fa	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 733f33faedb263d914163043b5242f0a.
Strike Allakore_746c9f8f	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 746c9f8f002fb8569d19cb2cdc1295ed.
Strike Allakore_750a3353	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 750a33531763724e8db051750a08cf99.

<b>Name</b>	<b>Description</b>
Strike Allakore_768a78b4	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 768a78b4b12efe721139c474fbf139f4.
Strike Allakore_80151f17	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 80151f17cd04b05f7765071c40215c40.
Strike Allakore_81444a9c	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is 81444a9c9f74be2c8ba32542bcc68bab.
Strike Allakore_a3d03ec0	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is a3d03ec08345e7cf02818122fc5b31f3.
Strike Allakore_a50d0d1b	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is a50d0d1bf9ab8291e986e59ebd92be14.
Strike Allakore_aa8b32b2	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is aa8b32b21dcf44a332f9c9d13af3cd7d.
Strike Allakore_ac69851a	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is ac69851a5144e0eb28923ca2e3b8cbe2.
Strike Allakore_b2cb036f	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is b2cb036f919d3cd003023c95c4bbb983.
Strike Allakore_b90a102f	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is b90a102fccedad57b06dc8fb6a58895b.

<b>Name</b>	<b>Description</b>
Strike Allakore_b99d788c	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is b99d788c4dcfd8cc7140e840bd8f5095.
Strike Allakore_bd378258	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is bd3782580c0ddbda2288b2d5d5a72258.
Strike Allakore_bd9d9a4b	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is bd9d9a4be3d93acf3228607b435a4828.
Strike Allakore_c48f0372	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is c48f0372aecf3a7c3d8fab599e7afcde.
Strike Allakore_c74e97cf	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is c74e97cf0086782ab8d22919b11f9c9d.
Strike Allakore_d355ff7b	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is d355ff7b4e022eff5c2b5a5aabae5ad0.
Strike Allakore_d72dfe82	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is d72dfe82b6072cb349120abdbd383aca.
Strike Allakore_df9b2ff8	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is df9b2ff8bd9164ae0f2c802c555d2c4f.
Strike Allakore_e6416904	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is e641690408faf6320fd7c820644ec889.

<b>Name</b>	<b>Description</b>
Strike Allakore_e78fa70b	This strike sends a malware sample known as Allakore. Allakore is a Remote Access Tool. This malware primarily used for spying and data exfiltration so it includes capabilities like keylogging, taking screenshots, upload/download files, and even take remote control of the victim's device. The MD5 hash of this Allakore sample is e78fa70b0e38c7c8c29048ceba2dd74.
Strike Ande Loader_1a321713	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is 1a321713876f764543d75859a4727b9a.
Strike Ande Loader_2885d0ab	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is 2885d0ab293d957f2a237a64f956d61a.
Strike Ande Loader_2a59f2a5	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is 2a59f2a51b96d9364e10182a063d9bec.
Strike Ande Loader_2e30e9db	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is 2e30e9db2016f9cb67d0f5ec4ca3d0a3.
Strike Ande Loader_48b6064b	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is 48b6064beec687fc110145cf7a19640d.
Strike Ande Loader_4c30ea43	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is 4c30ea433832fb13b5d7637d3b13bead.
Strike Ande Loader_64b690d3	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is 64b690d32216049b199234c5fc092e6f.

<b>Name</b>	<b>Description</b>
Strike Ande Loader_6ecd3d6c	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is 6ecd3d6c93cec7e7133af691c2c2225.
Strike Ande Loader_6f62e2ab	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is 6f62e2abb7558c83f2a4d3edefa05c7f.
Strike Ande Loader_97c880a2	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is 97c880a2514a9faaaa327e745a4c5c5c.
Strike Ande Loader_99d3b2eb	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is 99d3b2eb598775d41b18d57a9d1dc9ee.
Strike Ande Loader_9e447f72	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is 9e447f721d859407da88a8e6992e4aa0.
Strike Ande Loader_a5da69e6	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is a5da69e6c72a8759297415a0e30cbea8.
Strike Ande Loader_ac2940e6	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is ac2940e6619dbc4dbb1a096f657dd346.
Strike Ande Loader_b8f878d1	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is b8f878d1ee6a118f9eee4cf111193f53.

<b>Name</b>	<b>Description</b>
Strike Ande Loader_bcb0ed50	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is bcb0ed502a8275a23a9d627f319cb610.
Strike Ande Loader_e14efed3	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is e14efed36bb6870d65277776281dc3b3.
Strike Ande Loader_fb4c1a0a	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is fb4c1a0a6d525af1e3778e9e9ee48c7d.
Strike Ande Loader_ffcbdcec	This strike sends a malware sample known as Ande Loader. Blind Eagle also known as APT-C-36 is a threat actor that has recently been targeting Spanish speaking users in North America. These recent attacks include utilizing the malware Loader Ande Loader to deliver multiple payloads including the Remcos RAT and NjRAT. This sample is Ande Loader. The MD5 hash of this Ande Loader sample is ffcbdcec38e077448a87f5546dada7bd.
Strike AndroidRAT_0ac539e2	This strike sends a malware sample known as AndroidRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is AndroidRAT. The MD5 hash of this AndroidRAT sample is 0ac539e23e9befbbc96b874719fce50.
Strike AndroidRAT_a0e72ce4	This strike sends a malware sample known as AndroidRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is AndroidRAT. The MD5 hash of this AndroidRAT sample is a0e72ce4f88f7f8dcccce31db8ace8a2.
Strike AppLite_02cb6886	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 02cb688659724d8626e8ba2bfe4d1283.

<b>Name</b>	<b>Description</b>
Strike AppLite_049f1a2e	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 049f1a2e56a2a7c880b6dd36ef5a1410.
Strike AppLite_0a37d375	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 0a37d37587a295f4ad93d876852297a5.
Strike AppLite_0b35e159	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 0b35e15902a6d6f347dda13311476eb7.
Strike AppLite_0c4abdc8	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 0c4abdc8884ae185f1e0fc6aebed331e.
Strike AppLite_0e851208	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 0e8512084583e262f9ed533fda174ab6.
Strike AppLite_117d8c22	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 117d8c22241aa66d9cbbb362de6fb82.
Strike AppLite_128558fb	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 128558fb4617a6a95d0e9880a71ebb67.

<b>Name</b>	<b>Description</b>
Strike AppLite_16e936f7	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 16e936f77c43ff19ac3308e7ae3414fd.
Strike AppLite_173dda3b	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 173dda3ba226d71e38f6fa6a868259da.
Strike AppLite_1862fe71	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 1862fe712ae11b3443283b9969916985.
Strike AppLite_18cdcfca8	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 18cdcfca89e7613c003b0e98f4e327b5b.
Strike AppLite_1e52a7e0	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 1e52a7e0032e97ae867a945a2bf6551c.
Strike AppLite_1ea12742	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 1ea127424b8ab63801f8b437517a68a4.
Strike AppLite_1f21aee9	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 1f21aee9a7d724613a301e93f44ca31b.

<b>Name</b>	<b>Description</b>
Strike AppLite_1f7495ee	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 1f7495ee9825d7f77743e1ac2ce37a13.
Strike AppLite_202aa7f9	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 202aa7f9ef0b88a96f27a4362266f249.
Strike AppLite_2266a75b	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 2266a75b52d19ab41820307650fab362.
Strike AppLite_239498ff	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 239498ff472538e7a8380bae9a54e042.
Strike AppLite_2506cc9d	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 2506cc9d86fcb5134b8e802ded35ce12.
Strike AppLite_25ec0608	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 25ec0608969e7a60bada15b860ca66f5.
Strike AppLite_29554c53	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 29554c53052995a484a8b6f1b4146510.

<b>Name</b>	<b>Description</b>
Strike AppLite_29cdf7f9	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 29cdf7f9319707604345cd6d82e36b47.
Strike AppLite_2dde06b8	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 2dde06b8674a3bfd5b435560381f6c5f.
Strike AppLite_307ed00c	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 307ed00cfa1779194a5999f9601cae6f.
Strike AppLite_32afeb8a	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 32afeb8a25bd43d01bc142df28ead886.
Strike AppLite_33e2067d	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 33e2067da6325ec9a29c1e6788bcfded.
Strike AppLite_36532e46	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 36532e4613f7afcfc67ab2c5e33f013ff.
Strike AppLite_36ee80c6	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 36ee80c62ea2a152567840604f9a65bd.

<b>Name</b>	<b>Description</b>
Strike AppLite_370f8829	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 370f88291de979dcc7c9413e34223380.
Strike AppLite_3939a36a	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 3939a36a2f889d3d3846a456ed79b739.
Strike AppLite_3f0d93f4	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 3f0d93f4ccc85ffa1c3d44dea09b5bc5.
Strike AppLite_3f6ba5f6	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 3f6ba5f6bde27954be0c85ac85c43ee3.
Strike AppLite_3f86586b	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 3f86586b471c66f7638417043a03763a.
Strike AppLite_43323dda	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 43323dda747da5d355d7de3320e3edea.
Strike AppLite_44ec3195	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 44ec3195bcb54fb0baf289abd817bae8.

<b>Name</b>	<b>Description</b>
Strike AppLite_452710fc	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 452710fc96c5a3bf4d78fb6b77b3b3b9.
Strike AppLite_4617b681	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 4617b681b582b5d2f30f8770adc48d2d.
Strike AppLite_477303c1	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 477303c1161374d260e58a2a1c046495.
Strike AppLite_483054bd	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 483054bd15748a872b2de6b3b9f66034.
Strike AppLite_497a9320	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 497a932015780f31c0e3619231baa2f7.
Strike AppLite_4982e66f	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 4982e66fcc1ad470d0a93022b3c7dcc0.
Strike AppLite_4b316a5f	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 4b316a5f37a2183f9976a99cd31f3f9f.

<b>Name</b>	<b>Description</b>
Strike AppLite_4b5519db	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 4b5519db238cf4590407c966555bbe9c.
Strike AppLite_4c508b9d	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 4c508b9de40ddd994e87451dfa5a44f6.
Strike AppLite_4d2d8be6	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 4d2d8be66cefc3008f2ea85ea4f933d3.
Strike AppLite_4d4bde24	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 4d4bde24933214638df7fb62a80e94c7.
Strike AppLite_4f85ac46	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 4f85ac46bad0659436c86d072edc8d6b.
Strike AppLite_4fac403d	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 4fac403ddf4f150027e76284eda5c2e.
Strike AppLite_51d36416	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 51d364164b9a35b7c023d81ab53b0f1d.

<b>Name</b>	<b>Description</b>
Strike AppLite_551831e8	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 551831e86a10c761d3897419e3405f00.
Strike AppLite_56bf2dc0	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 56bf2dc05c8c90eadb398353fdb710bb.
Strike AppLite_5a45e6ff	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 5a45e6ffaacd0ac379c57090bb6bbb60.
Strike AppLite_5fec307f	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 5fec307f2999a7353dc5dad9e1231c6c.
Strike AppLite_61945574	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 61945574647d2f7c01fa523f4d76e6ee.
Strike AppLite_61f997af	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 61f997afa82707079c21c572ca0f182d.
Strike AppLite_62c14911	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 62c14911c9e00f41406aa1ab3753bdef.

<b>Name</b>	<b>Description</b>
Strike AppLite_644bb814	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 644bb8143e0d9cac863a38fc5b59396e.
Strike AppLite_653b58c2	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 653b58c2733ff3fdbd9fb451be3fdd855.
Strike AppLite_65b68850	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 65b688509c1c05d2bc2901a7855e0e44.
Strike AppLite_66df7c39	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 66df7c392e87c7ca287f09ef24fa1444.
Strike AppLite_6803ba86	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 6803ba86824e8d4730f9b631dc145dc9.
Strike AppLite_6a8edd52	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 6a8edd52675d2971d95d5151ae8fdf56.
Strike AppLite_6c9c6ab9	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 6c9c6ab9eafb8ac49def04517105152c.

<b>Name</b>	<b>Description</b>
Strike AppLite_7032ed34	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 7032ed34fc9d2394d974295a0bedd797.
Strike AppLite_703902dd	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 703902dd773351bdd609cc966ddb663e.
Strike AppLite_736e623e	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 736e623e2e85ec7b1360e9df07ab2fb8.
Strike AppLite_747c7b4b	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 747c7b4b634c32f4dfcfbcec3b230406.
Strike AppLite_7513b9c2	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 7513b9c2d67d3944a04cc085522d2f90.
Strike AppLite_76312d03	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 76312d033c7eb5fda48be1f73e702ef1.
Strike AppLite_774eed0b	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 774eed0b01e9febec2793ca8fd39b4ca.

<b>Name</b>	<b>Description</b>
Strike AppLite_77b741e5	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 77b741e5d1dabdf5309da628d15ed3a0.
Strike AppLite_781d5853	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 781d58538e2d740b1c01a620d5082c70.
Strike AppLite_786fee84	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 786fee84486a376ca63c4ff2325da101.
Strike AppLite_787b371b	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 787b371ba4a0732dd9806d29a1c0341b.
Strike AppLite_79fd4382	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 79fd43829c3e83b17cc0f7e7cebd15c2.
Strike AppLite_7ffcb948	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 7ffcb948061791cd427729fe0e177357.
Strike AppLite_810978af	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 810978afbd02e206dd05b8199ea2a1e9.

<b>Name</b>	<b>Description</b>
Strike AppLite_8444fb2a	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 8444fb2a33d7aa2bb7205555839d031.
Strike AppLite_844f26cb	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 844f26cb3e87514ebbdcc744312853ee2.
Strike AppLite_88d26f30	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 88d26f30bf87a4d4afe259bf0858ba02.
Strike AppLite_899db674	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 899db67405fac2249118a9cc72df78d2.
Strike AppLite_89a42453	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 89a4245390018c3d0736aa7fff83c9ec.
Strike AppLite_8a8a05d1	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 8a8a05d1eb3d041bf7de7d1a4347de58.
Strike AppLite_8aeba934	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 8aeba93492b1898bc5a73bab53d2fed9.

<b>Name</b>	<b>Description</b>
Strike AppLite_8b3366ac	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 8b3366acba1405dc95eda0a465ae293f.
Strike AppLite_8bdc1d48	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 8bdc1d486f57e6eb5a91d5e6784254b4.
Strike AppLite_8c27b8ef	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 8c27b8ef86085d3ae836e531f911f196.
Strike AppLite_8c5c591c	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 8c5c591ce6c1ccf51b00ea989e8d513b.
Strike AppLite_8cad79e3	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 8cad79e38f3a0fe8f5165531691f97d0.
Strike AppLite_8dfea9e3	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 8dfea9e3e7f038f7c0fa2129c93b9eeb.
Strike AppLite_8e03e900	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 8e03e90022214eda8f01ce735d8fe972.

<b>Name</b>	<b>Description</b>
Strike AppLite_92edb3cc	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 92edb3cc91a6b29c1b63f0416ae073ab.
Strike AppLite_9594729f	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 9594729f75d6b848980031db5575d271.
Strike AppLite_9683b6ec	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 9683b6ecc9bdb93a012eadd5fe1a3fd2.
Strike AppLite_993009c9	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 993009c900da786f27a1c9490c1fcf97.
Strike AppLite_9abcc9ac	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 9abcc9ac2a548f7da9fd296bd4bda1bf.
Strike AppLite_9bca475a	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 9bca475a728d9ccae923b8bbb20338df.
Strike AppLite_9f32c959	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 9f32c9598ef65928919885cdb42f6189.

<b>Name</b>	<b>Description</b>
Strike AppLite_9fe651f9	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is 9fe651f90953e7558da70f46bf807bb3.
Strike AppLite_a18da6b7	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is a18da6b7828b9bd886371801924c836a.
Strike AppLite_a7780316	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is a7780316b6b4ef800bec9a8c176245a9.
Strike AppLite_a86499ae	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is a86499ae9b3fae79e45663151eb3da9f.
Strike AppLite_a8fa0199	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is a8fa01995f63022d59e72fca525c1bdc.
Strike AppLite_aed6e039	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is aed6e039ac7b1de37cb5bcd31e007a7c.
Strike AppLite_b3225d6c	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is b3225d6c408e4ea7c28e44d0da7d6ad0.

<b>Name</b>	<b>Description</b>
Strike AppLite_b72fc97f	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is b72fc97f7d313106b509a90ddbc80c3b.
Strike AppLite_bd92d2d3	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is bd92d2d375bcb30e853702a6411d5fdf.
Strike AppLite_bf5284bd	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is bf5284bde7432eed1d3235e8f8c8a552.
Strike AppLite_bfd310e6	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is bfd310e6fb14023dd3cc9125cff2a22d.
Strike AppLite_c49c92f4	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is c49c92f4db80123c5e135d3d186ca7b7.
Strike AppLite_c530ab86	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is c530ab86b18d5c6679925a3dd3fb4418.
Strike AppLite_c8a20361	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is c8a20361bf491a0b2108fb27b55c637f.

<b>Name</b>	<b>Description</b>
Strike AppLite_c95248b2	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is c95248b21b3caf0a27c2ddf237460e09.
Strike AppLite_cab76022	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is cab76022c838b5ef334b1ed80ef94739.
Strike AppLite_cb71a7d5	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is cb71a7d571996bd6d989f7cb00056d83.
Strike AppLite_cccb3d0e	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is cccb3d0e7468948074464a496edb6025.
Strike AppLite_cf38315f	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is cf38315fb765e50310092f2b37f9a926.
Strike AppLite_cfbdb2846	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is cfbdb2846e01cf37e6907acc6539656c3.
Strike AppLite_cff1bf4d	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample iscff1bf4da3514aed61853124cf487b38.

<b>Name</b>	<b>Description</b>
Strike AppLite_d1b7e724	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is d1b7e7241390ba9c82f2d1a29bd3b34a.
Strike AppLite_d36b05dd	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is d36b05dd7a0ff63c7d69a71c3154ae96.
Strike AppLite_d6484a98	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is d6484a98a0a707e23ecab0a5fb8fb0ab.
Strike AppLite_d94cecc5	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is d94cecc512e2658319d95aa1b9ddfd9b.
Strike AppLite_d98c8480	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is d98c8480aa82af7027c151bbade657f1.
Strike AppLite_df2e2551	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is df2e25512953821661b4ab8a5688a9c8.
Strike AppLite_e0df402a	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is e0df402ae0da812ba559926084ce565b.

<b>Name</b>	<b>Description</b>
Strike AppLite_e3699cad	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is e3699cad111d4990a8738896a58b81c1.
Strike AppLite_e4c631e6	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is e4c631e6b63e3d2037fa0c959d52ffaf.
Strike AppLite_e67c5d39	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is e67c5d396ae9d97acc7f922ca39ccab2.
Strike AppLite_e6c96197	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is e6c96197eb41de926fe43d6721f01aaf.
Strike AppLite_e94c90f3	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is e94c90f3a89b0c3b971efbf97eff9609.
Strike AppLite_ea7074aa	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is ea7074aa96fc22c8a762a6f0b33e739b.
Strike AppLite_ebad9863	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is ebad9863c3be8e1db8753db8642e238e.

<b>Name</b>	<b>Description</b>
Strike AppLite_ed1693ec	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is ed1693ec88693c9384288e437e181ad6.
Strike AppLite_ed1dd47e	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is ed1dd47ee8ea4b6bb0d06837c5e96d70.
Strike AppLite_f661f0a6	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is f661f0a6bea508aa1625b4b271736fd7.
Strike AppLite_f80a46c7	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is f80a46c7bb8a3de2b117ee3d43115335.
Strike AppLite_f810c8bb	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is f810c8bb9ed0acb032cb3fe8eae68c7b.
Strike AppLite_f8effcac	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is f8effcac7bbc87d7b027310e42e0df9.
Strike AppLite_fa5638f9	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is fa5638f9e8fa078709529dd7cb335e6e.

<b>Name</b>	<b>Description</b>
Strike AppLite_fb04b1be	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is fb04b1be22c26c74a409cf6471611819.
Strike AppLite_fb7c0048	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is fb7c0048367dffecfbbedcb001f0728a.
Strike AppLite_fb8fabac	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is fb8fabacbc866b75a6db90b7f6a596c3.
Strike AppLite_fffc09d8	This strike sends a malware sample known as AppLite. AppLite malware is a new malware variant of the Antidot banking trojan. This malware is part of a mobile phishing campaign that targets Android devices. This app masquerades as several legitimate apps like Chrome and TikTok, and has capabilities ranging from banking credential theft, to full application and device take over. The MD5 hash of this AppLite sample is fffc09d8096d2692227f9c69f21876f7.
Strike AridSpy_0980b29b	This strike sends a malware sample known as AridSpy. AridSpy is a multi-stage Android malware. AridSpy is part of the Arid Viper attack campaigns targeting Android users. The malware infects the host device via download and installation of apps bundled with the malicious code. After ensuring security software isn't installed the malware will download the 1st stage payload that impersonates the Google Play store. From here a 2nd stage payload is downloaded and communication begins with the C2 server in which all of the device information can be uploaded. The MD5 hash of this AridSpy sample is 0980b29b5f52a36339ded0d62ec1af79.
Strike AridSpy_103e22b0	This strike sends a malware sample known as AridSpy. AridSpy is a multi-stage Android malware. AridSpy is part of the Arid Viper attack campaigns targeting Android users. The malware infects the host device via download and installation of apps bundled with the malicious code. After ensuring security software isn't installed the malware will download the 1st stage payload that impersonates the Google Play store. From here a 2nd stage payload is downloaded and communication begins with the C2 server in which all of the device information can be uploaded. The MD5 hash of this AridSpy sample is 103e22b050bdac39a80aac2c2831902d.

<b>Name</b>	<b>Description</b>
Strike AridSpy_24ac2a35	This strike sends a malware sample known as AridSpy. AridSpy is a multi-stage Android malware. AridSpy is part of the Arid Viper attack campaigns targeting Android users. The malware infects the host device via download and installation of apps bundled with the malicious code. After ensuring security software isn't installed the malware will download the 1st stage payload that impersonates the Google Play store. From here a 2nd stage payload is downloaded and communication begins with the C2 server in which all of the device information can be uploaded. The MD5 hash of this AridSpy sample is 24ac2a350a3c6aeb2e75413eb7c57ef1.
Strike AridSpy_2f5d39c3	This strike sends a malware sample known as AridSpy. AridSpy is a multi-stage Android malware. AridSpy is part of the Arid Viper attack campaigns targeting Android users. The malware infects the host device via download and installation of apps bundled with the malicious code. After ensuring security software isn't installed the malware will download the 1st stage payload that impersonates the Google Play store. From here a 2nd stage payload is downloaded and communication begins with the C2 server in which all of the device information can be uploaded. The MD5 hash of this AridSpy sample is 2f5d39c31808ecf71b333818887d2f17.
Strike AridSpy_68913836	This strike sends a malware sample known as AridSpy. AridSpy is a multi-stage Android malware. AridSpy is part of the Arid Viper attack campaigns targeting Android users. The malware infects the host device via download and installation of apps bundled with the malicious code. After ensuring security software isn't installed the malware will download the 1st stage payload that impersonates the Google Play store. From here a 2nd stage payload is downloaded and communication begins with the C2 server in which all of the device information can be uploaded. The MD5 hash of this AridSpy sample is 68913836ca1145bff0e2c08e4ae2d650.
Strike AridSpy_7269751a	This strike sends a malware sample known as AridSpy. AridSpy is a multi-stage Android malware. AridSpy is part of the Arid Viper attack campaigns targeting Android users. The malware infects the host device via download and installation of apps bundled with the malicious code. After ensuring security software isn't installed the malware will download the 1st stage payload that impersonates the Google Play store. From here a 2nd stage payload is downloaded and communication begins with the C2 server in which all of the device information can be uploaded. The MD5 hash of this AridSpy sample is 7269751abac507dd0305b89047e6851a.
Strike AridSpy_a2d0a2bb	This strike sends a malware sample known as AridSpy. AridSpy is a multi-stage Android malware. AridSpy is part of the Arid Viper attack campaigns targeting Android users. The malware infects the host device via download and installation of apps bundled with the malicious code. After ensuring security software isn't installed the malware will download the 1st stage payload that impersonates the Google Play store. From here a 2nd stage payload is downloaded and communication begins with the C2 server in which all of the device information can be uploaded. The MD5 hash of this AridSpy sample is a2d0a2bb4d63b11cdcb8f317d54f1383.

<b>Name</b>	<b>Description</b>
Strike AridViper_13408d1a	This strike sends a polymorphic malware sample known as Arid Viper. Arid Viper is an espionage-driven group that delivers attacks targeting Middle Eastern Android users through social engineering techniques. Their primary tool is SpyC23, a family of Android malware disguised as legitimate applications. It steals sensitive information from the device, disables security notifications, and deploys additional malware. 'com.apps.sklite' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 13408d1a4e3d127b786a0379a8739d04.
Strike AridViper_1bba05c0	This strike sends a polymorphic malware sample known as Arid Viper. Arid Viper is an espionage-driven group that delivers attacks targeting Middle Eastern Android users through social engineering techniques. Their primary tool is SpyC23, a family of Android malware disguised as legitimate applications. It steals sensitive information from the device, disables security notifications, and deploys additional malware. 'com.apps.sklite' is the package name of the malware sample. Constant strings in the code has been encrypted. The MD5 hash of this malware sample is 1bba05c04fde9b44a2243ef965367e45.
Strike AridViper_decf384d	This strike sends a malware sample known as Arid Viper. Arid Viper is an espionage-driven group that delivers attacks targeting Middle Eastern Android users through social engineering techniques. Their primary tool is SpyC23, a family of Android malware disguised as legitimate applications. It steals sensitive information from the device, disables security notifications, and deploys additional malware. 'com.apps.sklite' is the package name of the malware sample. The MD5 hash of this malware sample is decf384d8c0a2a036abff47331d6ab98.
Strike Arkei_00befcd0	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is 00befcd06035d0bb7f4256c22145e077.
Strike Arkei_05fdf040	This strike sends a polymorphic malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Arkei sample is 05fdf0408dd7e5ba480e1d62a5843466.
Strike Arkei_0eed4e7b	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is 0eed4e7bb0e7e3e84b119e1e623b427f.
Strike Arkei_0f6b5657	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is 0f6b5657da0ffc54ac13fc4ce414cf4d.
Strike Arkei_10a38d0a	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is 10a38d0ae84dc819e4e91bdc307ed3dc.

<b>Name</b>	<b>Description</b>
Strike Arkei_15712005	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is 157120055c4f2922c52bd5efebf090b7.
Strike Arkei_167af7b6	This strike sends a polymorphic malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The binary has random bytes appended at the end of the file. The MD5 hash of this Arkei sample is 167af7b6ea9eccb08d2071e78ded9c47.
Strike Arkei_1df03fa3	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is 1df03fa342958648b48b9369be8ff9b3.
Strike Arkei_249acf68	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is 249acf68b841fb953571ab1ef246b497.
Strike Arkei_2da317a6	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is 2da317a6e7600b40a419eb788608191f.
Strike Arkei_307dbc09	This strike sends a polymorphic malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Arkei sample is 307dbc0918a2ee073c645d4882f3552b.
Strike Arkei_3dc6ef89	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is 3dc6ef8923433a89af4bab1e54ccdc02.
Strike Arkei_55a7ecd0	This strike sends a polymorphic malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The binary has random bytes appended at the end of the file. The MD5 hash of this Arkei sample is 55a7ecd0c065b3f57347ab2737a44295.
Strike Arkei_568b477b	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is 568b477bb674e07132eefd19d5c45a56.
Strike Arkei_8cd00f75	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is 8cd00f759280f034e02f6e58720bda7d.
Strike Arkei_8edaee6d	This strike sends a polymorphic malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Arkei sample is 8edaee6d0a70ed278c0dbc435d957d31.

<b>Name</b>	<b>Description</b>
Strike Arkei_a4b38793	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is a4b387930e6081c7739f28bf77f2ce4a.
Strike Arkei_b119465c	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is b119465c150e0173b6b184448b5cf088.
Strike Arkei_cf64deaa	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is cf64deaaefbc00ff53e14bcfd9a86e4.
Strike Arkei_d73ec126	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is d73ec12627a319b61bf8f248c6516262.
Strike Arkei_e63543c9	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is e63543c93b4d214c80e8c589582a7acb.
Strike Arkei_f2ef1fc0	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is f2ef1fc097d3805815d0f1db06db6c2f.
Strike Arkei_f3a4bb8f	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is f3a4bb8fca6d399c3a1a9ff750c48441.
Strike Arkei_f52cb089	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is f52cb0892baaab89703ab9d4f42a5483.
Strike Arkei_f7359ffd	This strike sends a malware sample known as Arkei. Arkei is an information-stealing malware that collects passwords, credit card information and web browser cookies. The MD5 hash of this Arkei sample is f7359ffdc1b165863867f00046c03bd1.
Strike AsukaStealer_08c505ac	This strike sends a polymorphic malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The binary has been packed using upx packer, with the default options. The MD5 hash of this AsukaStealer sample is 08c505ac90892374c7f301829a8d326a.
Strike AsukaStealer_0e270dbe	This strike sends a polymorphic malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The binary has random bytes appended at the end of the file. The MD5 hash of this AsukaStealer sample is 0e270dbe5d6d8007f6eaeb376ab2da74.

<b>Name</b>	<b>Description</b>
Strike AsukaStealer_1494c8bc	This strike sends a malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The MD5 hash of this AsukaStealer sample is 1494c8bc32576cb008c33d6f0fd1e842.
Strike AsukaStealer_1a1634af	This strike sends a polymorphic malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The binary has the timestamp field updated in the PE file header. The MD5 hash of this AsukaStealer sample is 1a1634af7b1ba52d1283f52ed899693e.
Strike AsukaStealer_20017810	This strike sends a malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The MD5 hash of this AsukaStealer sample is 20017810fba85ef8ac6e4230d0e67a07.
Strike AsukaStealer_21fe44da	This strike sends a polymorphic malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this AsukaStealer sample is 21fe44daba3755033e1b6708f544b57b.
Strike AsukaStealer_28b7d6b0	This strike sends a malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The MD5 hash of this AsukaStealer sample is 28b7d6b0a793d772c953f529742ca91f.
Strike AsukaStealer_2d2b66d9	This strike sends a malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The MD5 hash of this AsukaStealer sample is 2d2b66d90495c1236f2e557172bf0f1c.
Strike AsukaStealer_2de37ffc	This strike sends a malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The MD5 hash of this AsukaStealer sample is 2de37ffcae86c673de3cd2ee5e2ad3b1.
Strike AsukaStealer_34107ceb	This strike sends a polymorphic malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The binary has random bytes appended at the end of the file. The MD5 hash of this AsukaStealer sample is 34107cebda9fc2d902c531377b38530d.

<b>Name</b>	<b>Description</b>
Strike AsukaStealer_371e14f7	This strike sends a malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The MD5 hash of this AsukaStealer sample is 371e14f7e146ff22cb9ebe2f78cbfb7f.
Strike AsukaStealer_4a4943d1	This strike sends a polymorphic malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The binary has the signature removed in the PE file format. The MD5 hash of this AsukaStealer sample is 4a4943d11594b94332f9e6e79f509f6e.
Strike AsukaStealer_515e77da	This strike sends a polymorphic malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this AsukaStealer sample is 515e77da1ddd282b054a40a0c93fb9e2.
Strike AsukaStealer_7ce0bd10	This strike sends a malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The MD5 hash of this AsukaStealer sample is 7ce0bd101d349bc88b668e380093e1a9.
Strike AsukaStealer_7da46b7c	This strike sends a polymorphic malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The binary has the debug flag removed in the PE file format. The MD5 hash of this AsukaStealer sample is 7da46b7c9e2053d1f0e7ed588a58faf3.
Strike AsukaStealer_845dc635	This strike sends a polymorphic malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this AsukaStealer sample is 845dc6356a8e7ffc6fc21e30ca54478a.
Strike AsukaStealer_8580a630	This strike sends a polymorphic malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this AsukaStealer sample is 8580a6307bb564e8b3613b542718872d.
Strike AsukaStealer_9ce2a046	This strike sends a malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The MD5 hash of this AsukaStealer sample is 9ce2a046a0698212c2963f2df91ff2e1.

<b>Name</b>	<b>Description</b>
Strike AsukaStealer_9db4859f	This strike sends a polymorphic malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The binary has been packed using upx packer, with the default options. The MD5 hash of this AsukaStealer sample is 9db4859f339604dc474eb87407535480.
Strike AsukaStealer_e860e2e9	This strike sends a polymorphic malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this AsukaStealer sample is e860e2e91ffe0db44e044bb777cb884e.
Strike AsukaStealer_e9dda8cc	This strike sends a malware sample known as AsukaStealer. AsukaStealer is infostealer malware that is offered as Malware-as-a-services (MaaS). It is designed to collect data from browsers, Discord tokens, FileZilla and Telegram sessions, crypto wallets, and desktop screenshots. The MD5 hash of this AsukaStealer sample is e9dda8ccde5385e8d0a7f0bdc361e51d.
Strike AsyncRAT_07f3f073	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 07f3f073391f7308ca1c7ef54d6c5656.
Strike AsyncRAT_0a80a592	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 0a80a592d407a2a8b8b318286dc30769.
Strike AsyncRAT_0a82a328	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 0a82a32801a0a2c1bcf4371a4a582f5e.

<b>Name</b>	<b>Description</b>
Strike AsyncRAT_55a0c7d6	<p>This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 55a0c7d6356dfa4c7b45ef03caf2ac75.</p>
Strike AsyncRAT_5b02fac6	<p>This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 5b02fac6ed22c683e36715e3c7ae05fc.</p>
Strike AsyncRAT_5ee0d653	<p>This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 5ee0d653dba5a4308a7bf5da642daff1.</p>
Strike AsyncRAT_61b7507a	<p>This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 61b7507a6814e81cda6b57850f9f31da.</p>
Strike AsyncRAT_67fefafa4b	<p>This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 67fefafa4bc5ee224e814bea6602399df8.</p>

<b>Name</b>	<b>Description</b>
Strike AsyncRAT_73bd7a8e	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 73bd7a8efb5d7150633432bde16cd980.
Strike AsyncRAT_790562ce	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 790562cefbb2c6b9d890b6d2b4adc548.
Strike AsyncRAT_825a5d12	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 825a5d120ab305b5e12731307a0bee63.
Strike AsyncRAT_8d019622	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 8d01962215ddfe754b725fa9f835b2d6.
Strike AsyncRAT_94719304	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 94719304694a573b087d7efdd8ab8eed.

<b>Name</b>	<b>Description</b>
Strike AsyncRAT_9b1b21fe	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is 9b1b21fe9b8ab2fb386dd5794c272baf.
Strike AsyncRAT_a31191ca	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is a31191ca8fe50b0a70eb48b82c4d6f39.
Strike AsyncRAT_ac12d457	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is ac12d457d3ee177af8824cdc1de47f2a.
Strike AsyncRAT_b29edf77	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is b29edf77f9af40aa7e5387f722d4e32.
Strike AsyncRAT_b4323259	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is b4323259d83bf99fd6f029a3c0d7e272.

<b>Name</b>	<b>Description</b>
Strike AsyncRAT_c0926666	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is c0926666ee71ade24e0e5f889cc8199.
Strike AsyncRAT_c2ce2c2a	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is c2ce2c2acb3b2f2ac33f459b850ba40d.
Strike AsyncRAT_c68996a7	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is c68996a7db8547fcbf2f3fd82a5e80ca.
Strike AsyncRAT_d4abb12d	This strike sends a malware sample known as AsyncRAT. AsyncRAT is a malware that uses WSF script format and is distributed through compressed (.zip) files via email URLs. The malware exhibits sophisticated evasion techniques by disguising itself within a .jpg file. Upon execution, it deploys a series of scripts, including Visual Basic, PowerShell, and a final .NET binary (AsyncRAT). Key capabilities of the malware involve persistence through scheduled tasks and registry entries, information exfiltration encompassing computer details, browser user data, and cryptocurrency wallet information. The C2 server, encrypted within the file, orchestrates data exfiltration. The MD5 hash of this AsyncRAT sample is d4abb12d79d42b0f392451c49cbe6733.
Strike AuKill_42bc883e	This strike sends a malware sample known as AuKill. AuKill is a defensive evasion tool that takes advantage of a legitimate but outdated driver used in the Process Explorer tool to disable EDR processes. This tool has been seen in conjunction with the deployment of the Medusa Locker ransomware and the Lockbit ransomware. The MD5 hash of this AuKill sample is 42bc883e7a31b011d2687eba178c2525.

<b>Name</b>	<b>Description</b>
Strike AuKill_811bd70a	This strike sends a malware sample known as AuKill. AuKill is a defensive evasion tool that takes advantage of a legitimate but outdated driver used in the Process Explorer tool to disable EDR processes. This tool has been seen in conjunction with the deployment of the Medusa Locker ransomware and the Lockbit ransomware. The MD5 hash of this AuKill sample is 811bd70aa6d099716b49794870c07b7d.
Strike BQTLock_058a1dbf	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is 058a1dbfa03cac6cc67d34a4dcc69445.
Strike BQTLock_110df495	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is 110df49522d46b612a28bafbdff3405c.
Strike BQTLock_3478194a	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is 3478194a509ae4d2f0a31435952b27bc.
Strike BQTLock_69e6fa25	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is 69e6fa25e66c23121826805bbcb890ac.
Strike BQTLock_84c7bfb0	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is 84c7bfb0e243dd99b674e48701acob6b.

<b>Name</b>	<b>Description</b>
Strike BQTLock_9569c863	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is 9569c8631bcd37da1a5048d979362804.
Strike BQTLock_972b1677	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is 972b1677621bbdc45ef61c56cd9909d2.
Strike BQTLock_a441e0a2	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is a441e0a25276952bb4fa2f29e06fc209.
Strike BQTLock_a6d91094	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is a6d91094a222da6576260abf52a07b79.
Strike BQTLock_acf3b7f2	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is acf3b7f2f07f5d04083f99b82eb0c8ba.
Strike BQTLock_b098f677	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is b098f67726a4a3f7277b3f41a86d503c.

<b>Name</b>	<b>Description</b>
Strike BQTLock_bc8cc3ca	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is bc8cc3ca2a45ebb934cd71218d9b56b3.
Strike BQTLock_c34d690b	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is c34d690bbe1f9dc78066c881e3596505.
Strike BQTLock_d6476590	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is d647659069d09b59a0e5d3608df314b2.
Strike BQTLock_d6cb9f18	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is d6cb9f18705c34c515dbfd59c4015576.
Strike BQTLock_dae6729c	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is dae6729cc3bfcbd700fc7e46818aada2.
Strike BQTLock_e73abc48	This strike sends a malware sample known as BQTLock. BQTLock is a ransomware that encrypts files on the victim's system and demands a ransom to decrypt them. It is delivered via phishing emails, malicious downloads, or exploit kits. Once executed, BQTLock encrypts the victim's files using AES-256 encryption and changes the filenames to ".bqt" extension. Its key capabilities include encryption of files, changing file extensions, and demanding a ransom in exchange for decryption. The MD5 hash of this BQTLock sample is e73abc48015c54214b2edae4a6d1ed25.

<b>Name</b>	<b>Description</b>
Strike BabbleLoader_30525477	This strike sends a malware sample known as BabbleLoader. BabbleLoader is a malware loader that is designed to bypass antivirus and sandbox environments to inject the malware into memory. This loader includes lots of junk code and ways to confuse and mislead AI detection mechanisms. The MD5 hash of this BabbleLoader sample is 30525477955ce3dc73af96fbf4dcdd42.
Strike BabbleLoader_46f556b2	This strike sends a malware sample known as BabbleLoader. BabbleLoader is a malware loader that is designed to bypass antivirus and sandbox environments to inject the malware into memory. This loader includes lots of junk code and ways to confuse and mislead AI detection mechanisms. The MD5 hash of this BabbleLoader sample is 46f556b28535ffd8ed4ae44eb1d9a3b2.
Strike BabbleLoader_5d31204e	This strike sends a malware sample known as BabbleLoader. BabbleLoader is a malware loader that is designed to bypass antivirus and sandbox environments to inject the malware into memory. This loader includes lots of junk code and ways to confuse and mislead AI detection mechanisms. The MD5 hash of this BabbleLoader sample is 5d31204e8c9a6e35d5534a730781c691.
Strike BabbleLoader_63f4bd22	This strike sends a malware sample known as BabbleLoader. BabbleLoader is a malware loader that is designed to bypass antivirus and sandbox environments to inject the malware into memory. This loader includes lots of junk code and ways to confuse and mislead AI detection mechanisms. The MD5 hash of this BabbleLoader sample is 63f4bd224289327bea085cb2e16cea49.
Strike BabbleLoader_7db7cc8f	This strike sends a malware sample known as BabbleLoader. BabbleLoader is a malware loader that is designed to bypass antivirus and sandbox environments to inject the malware into memory. This loader includes lots of junk code and ways to confuse and mislead AI detection mechanisms. The MD5 hash of this BabbleLoader sample is 7db7cc8f9bac5ee1a27f9ea7d4e75f5c.
Strike BabbleLoader_a1e2907b	This strike sends a malware sample known as BabbleLoader. BabbleLoader is a malware loader that is designed to bypass antivirus and sandbox environments to inject the malware into memory. This loader includes lots of junk code and ways to confuse and mislead AI detection mechanisms. The MD5 hash of this BabbleLoader sample is a1e2907beb8e073c75eaff5fc4dd732.
Strike BabbleLoader_dc5944bc	This strike sends a malware sample known as BabbleLoader. BabbleLoader is a malware loader that is designed to bypass antivirus and sandbox environments to inject the malware into memory. This loader includes lots of junk code and ways to confuse and mislead AI detection mechanisms. The MD5 hash of this BabbleLoader sample is dc5944bc1a3c90bc6d790e56d2faa026.
Strike BabbleLoader_dfc7d90f	This strike sends a malware sample known as BabbleLoader. BabbleLoader is a malware loader that is designed to bypass antivirus and sandbox environments to inject the malware into memory. This loader includes lots of junk code and ways to confuse and mislead AI detection mechanisms. The MD5 hash of this BabbleLoader sample is dfc7d90fcfd68da15d0552e76f6981972.
Strike BabbleLoader_ef954119	This strike sends a malware sample known as BabbleLoader. BabbleLoader is a malware loader that is designed to bypass antivirus and sandbox environments to inject the malware into memory. This loader includes lots of junk code and ways to confuse and mislead AI detection mechanisms. The MD5 hash of this BabbleLoader sample is ef95411945330db1907508d38bc373ac.

<b>Name</b>	<b>Description</b>
Strike Babuk Locker_024382ee	This strike sends a malware sample known as Babuk Locker. Babuk is a ransomware that first started appearing in early 2021. Recently a tool that was used in the creation of these ransomware samples has been detected in other attacks and is being called Babuk Locker. The MD5 hash of this Babuk Locker sample is 024382eef9abab8edd804548f94b78fc.
Strike Babuk Locker_4161cbe9	This strike sends a malware sample known as Babuk Locker. Babuk is a ransomware that first started appearing in early 2021. Recently a tool that was used in the creation of these ransomware samples has been detected in other attacks and is being called Babuk Locker. The MD5 hash of this Babuk Locker sample is 4161cbe9722d98ffe53636e9efa874ca.
Strike Babuk Locker_567c8369	This strike sends a malware sample known as Babuk Locker. Babuk is a ransomware that first started appearing in early 2021. Recently a tool that was used in the creation of these ransomware samples has been detected in other attacks and is being called Babuk Locker. The MD5 hash of this Babuk Locker sample is 567c8369e6ab695c9d65a629d6f45710.
Strike Babuk Locker_61bf40aa	This strike sends a polymorphic malware sample known as Babuk Locker. Babuk is a ransomware that first started appearing in early 2021. Recently a tool that was used in the creation of these ransomware samples has been detected in other attacks and is being called Babuk Locker. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Babuk Locker sample is 61bf40aa7be7bac60efcec70058af30b.
Strike Babuk Locker_a8c465b9	This strike sends a polymorphic malware sample known as Babuk Locker. Babuk is a ransomware that first started appearing in early 2021. Recently a tool that was used in the creation of these ransomware samples has been detected in other attacks and is being called Babuk Locker. The binary has the debug flag removed in the PE file format. The MD5 hash of this Babuk Locker sample is a8c465b971bb6ccfc517cf132a97f16d.
Strike Babuk Locker_b8e5bd86	This strike sends a malware sample known as Babuk Locker. Babuk is a ransomware that first started appearing in early 2021. Recently a tool that was used in the creation of these ransomware samples has been detected in other attacks and is being called Babuk Locker. The MD5 hash of this Babuk Locker sample is b8e5bd86046b596d8cf43843f433bb5d.
Strike Babuk Locker_cafe07d8	This strike sends a malware sample known as Babuk Locker. Babuk is a ransomware that first started appearing in early 2021. Recently a tool that was used in the creation of these ransomware samples has been detected in other attacks and is being called Babuk Locker. The MD5 hash of this Babuk Locker sample is cafe07d8c34108007372bd8df42d9ef9.
Strike Babuk Locker_cb95970a	This strike sends a polymorphic malware sample known as Babuk Locker. Babuk is a ransomware that first started appearing in early 2021. Recently a tool that was used in the creation of these ransomware samples has been detected in other attacks and is being called Babuk Locker. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Babuk Locker sample is cb95970ab2c06f8695a4741fe055ec25.

<b>Name</b>	<b>Description</b>
Strike Babuk Locker_d6fc9e99	This strike sends a malware sample known as Babuk Locker. Babuk is a ransomware that first started appearing in early 2021. Recently a tool that was used in the creation of these ransomware samples has been detected in other attacks and is being called Babuk Locker. The MD5 hash of this Babuk Locker sample is d6fc9e993c69aceb7a5501641fc823fa.
Strike Babuk Locker_dfaa9121	This strike sends a malware sample known as Babuk Locker. Babuk is a ransomware that first started appearing in early 2021. Recently a tool that was used in the creation of these ransomware samples has been detected in other attacks and is being called Babuk Locker. The MD5 hash of this Babuk Locker sample is dfaa9121f4165a9f38a8406d82f0ab71.
Strike Babuk Locker_eacfeff2	This strike sends a malware sample known as Babuk Locker. Babuk is a ransomware that first started appearing in early 2021. Recently a tool that was used in the creation of these ransomware samples has been detected in other attacks and is being called Babuk Locker. The MD5 hash of this Babuk Locker sample is eacfeff2add22da202bc6ba34308989e.
Strike Babuk Locker_ebe7bf69	This strike sends a malware sample known as Babuk Locker. Babuk is a ransomware that first started appearing in early 2021. Recently a tool that was used in the creation of these ransomware samples has been detected in other attacks and is being called Babuk Locker. The MD5 hash of this Babuk Locker sample is ebe7bf69eceb80d155d7a16b8c61e15c.
Strike Babuk Locker_f0d4c7d3	This strike sends a malware sample known as Babuk Locker. Babuk is a ransomware that first started appearing in early 2021. Recently a tool that was used in the creation of these ransomware samples has been detected in other attacks and is being called Babuk Locker. The MD5 hash of this Babuk Locker sample is f0d4c7d334633a72a3c7bd722e12c378.
Strike Babuk_0d0bc6f8	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is 0d0bc6f8144b4d3f3b80654b4fd8403a.
Strike Babuk_0f5f2290	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is 0f5f2290a30c8f0f33f39a4513794806.
Strike Babuk_1177aed7	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is 1177aed7c7e035e47af41a009eaaf020.

<b>Name</b>	<b>Description</b>
Strike Babuk_1799f830	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is 1799f8305930359699524757cbde2381.
Strike Babuk_19c4f4e3	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is 19c4f4e3eb499b4049c76546c99e0c10.
Strike Babuk_24532b52	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is 24532b52054bc1a848e47d917b4cc0a9.
Strike Babuk_4aa36591	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is 4aa36591efdc8bfcdde338972be9d90.
Strike Babuk_4b9bb8a7	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is 4b9bb8a7204b28332635f342b8ffdceb.
Strike Babuk_4e2a2080	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is 4e2a208090fcf8ce27d696ef15750d32.
Strike Babuk_5bf3dfab	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is 5bf3dfab3aac314adaa400a317987c82.

<b>Name</b>	<b>Description</b>
Strike Babuk_6ccb3ad5	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is 6ccb3ad50f52601d254f9c5b47f35e99.
Strike Babuk_7de7717e	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is 7de7717e90bb9aa2ad0e76e29994cf3f.
Strike Babuk_87b3f09a	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is 87b3f09aa41bad9d87c5cd17c1a0edfa.
Strike Babuk_8f84941f	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is 8f84941f03bc4a9f2633a283770e780b.
Strike Babuk_b6c46c1b	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is b6c46c1bd6ea86beae25c77d05280d59.
Strike Babuk_d229af68	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is d229af68c9896935edf632c2cc1adefc.
Strike Babuk_d615b6a4	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is d615b6a427256ebf1c132038aef19079.

<b>Name</b>	<b>Description</b>
Strike Babuk_dcc7371a	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is dcc7371a1bb7380221bc0d48b85d99b8.
Strike Babuk_e5a972cc	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is e5a972cc589109be1aae14cdb5fd6984.
Strike Babuk_f59c756a	This strike sends a malware sample known as Babuk. Babuk is a ransomware that first started appearing in early 2021. Recently a Babuk variant has surfaced in some multi-staged Ransom attacks from RA World. Some new updates to the variant include changes to the mutex name and ransom note filename. They also changed the encrypted extension and added more paths and filenames to exclude during the encryption process The MD5 hash of this Babuk sample is f59c756a517c9db12aaa35cdd0c4fbaf.
Strike BadSpace_003f4222	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 003f42221d4345a036554e3a5bc07252.
Strike BadSpace_00cf06f1	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 00cf06f175b845aa0d238d85663c07ad.
Strike BadSpace_039ff182	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 039ff182524d1f3c109869d5bee699a1.

<b>Name</b>	<b>Description</b>
Strike BadSpace_03fe551e	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 03fe551e88e7259c60002b4e1417c5a8.
Strike BadSpace_0454ef3f	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 0454ef3fc5d68efd450c7f29ff65fb28.
Strike BadSpace_045aa3f2	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 045aa3f2878ffca7925236fe00078fe6.
Strike BadSpace_07b8d434	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 07b8d4345a03d4ad26d9cdbd54cfecce.
Strike BadSpace_094e76d5	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 094e76d5331d94a02584dd7fd3d795ae.
Strike BadSpace_0cc4f62d	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 0cc4f62dae162f4f1ffa206207d8469a.

<b>Name</b>	<b>Description</b>
Strike BadSpace_0d6d19ee	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 0d6d19eeb517cfa45c285a28860fc941.
Strike BadSpace_0d7f58cb	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 0d7f58cb43f59d78fdb10627835e5977.
Strike BadSpace_0e43f2d8	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 0e43f2d82d99940168a02c21933c1756.
Strike BadSpace_12aa84e2	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 12aa84e2e56ae684d211679072695906.
Strike BadSpace_16953377	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 16953377c0ddd20f70ade252c0a8c41f.
Strike BadSpace_16ca38f2	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 16ca38f2b8364dd2ff051473ad138684.

<b>Name</b>	<b>Description</b>
Strike BadSpace_18ff7d29	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 18ff7d29a2beb92634eab27f2b39ceec.
Strike BadSpace_1ac17baf	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 1ac17baf9e0214f3fb270afa7a871153.
Strike BadSpace_1b7b6fb1	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 1b7b6fb1a99996587a3c20ee9c390a9c.
Strike BadSpace_1b7f494c	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 1b7f494c383385d9f76d17e5a9d757d3.
Strike BadSpace_1e327a54	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 1e327a54d1d87af79bf04b1776a8c2af.
Strike BadSpace_1f2912c0	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 1f2912c0c12b316023061de20ee3cc55.

<b>Name</b>	<b>Description</b>
Strike BadSpace_20274d81	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 20274d8185a2c83ee2d05ddb4caf6fe66.
Strike BadSpace_21382f8c	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 21382f8cef1c83b59c2568deaf610d34.
Strike BadSpace_2492aca3	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 2492aca399dfaf75e761586844734980.
Strike BadSpace_2642e28a	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 2642e28a1389924688b026619ae1ff49.
Strike BadSpace_26ebc6ae	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 26ebc6ae034edba997327852734db397.
Strike BadSpace_27b9ed14	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 27b9ed14b36d3aa75ada1674f16de359.

<b>Name</b>	<b>Description</b>
Strike BadSpace_29a6a816	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 29a6a8168d2c83d516964ace53458cff.
Strike BadSpace_2a463fe7	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 2a463fe704d5fbd299fa3315ea13b932.
Strike BadSpace_2c9aefc2	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 2c9aefc29c58618f86cf2ea1cd9c132f.
Strike BadSpace_3368a6df	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 3368a6dfd36f34671974b1e43521bf84.
Strike BadSpace_33cea9af	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 33cea9af8f22e5048b96413dc238c492.
Strike BadSpace_342dc118	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 342dc118538238a22829e7ceaf68d4ac.

<b>Name</b>	<b>Description</b>
Strike BadSpace_36039d4d	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 36039d4d4ec73620db0835201b85fc6e.
Strike BadSpace_3746c798	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 3746c798fa14f67d2426def475bc23a6.
Strike BadSpace_3849f4bc	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 3849f4bcef666a762e5f2c80c526f20e.
Strike BadSpace_389b784c	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 389b784c2ce97c05465da71cecd03c9b.
Strike BadSpace_3c7511cc	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 3c7511cc20744b39290929ee13249a03.
Strike BadSpace_3c8c64c7	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 3c8c64c782fb70528f45446f61cd5e5.

<b>Name</b>	<b>Description</b>
Strike BadSpace_3c90fd1d	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this BadSpace sample is 3c90fd1d6857aaeb535515b569631a71.
Strike BadSpace_3dab3a34	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 3dab3a340acdad73f5551715e76624eb.
Strike BadSpace_404ab87b	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 404ab87bbf07bd21c8a2438c22e77649.
Strike BadSpace_417119be	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 417119be6153068e59bc0e9a85c0c0ee.
Strike BadSpace_42a14390	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 42a1439065f37691796551faa853d88.
Strike BadSpace_4594f36c	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 4594f36c836442205c358013ce523c12.

<b>Name</b>	<b>Description</b>
Strike BadSpace_4599bd73	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 4599bd73b872c3691f67c9d9737daf52.
Strike BadSpace_460a2257	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 460a22575015815018897aaa542fd49b.
Strike BadSpace_47a08e51	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 47a08e518858c0813cdb1560b7032a84.
Strike BadSpace_4890bb49	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 4890bb490ed2196d915dc0ecea163bb.
Strike BadSpace_4b446163	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 4b44616333f1b1caeb4f28b023a69cd8.
Strike BadSpace_4ba17f3b	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 4ba17f3bb4e7473a7e63a9cb7d92d5dd.

<b>Name</b>	<b>Description</b>
Strike BadSpace_4caee169	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 4caee169f0c43247d27b60d8fe2ed78f.
Strike BadSpace_4d7407f6	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 4d7407f6b08c14f30a0afaa37999664f.
Strike BadSpace_506af984	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 506af98423364e39f4152dee027e3bdd.
Strike BadSpace_518e19ec	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 518e19ec607e64773dd76ca99a18017d.
Strike BadSpace_53094e21	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 53094e21d2782a8dc358334a9c7e547a.
Strike BadSpace_553844ba	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 553844baa97e06e37a55baf0652a7c7a.

<b>Name</b>	<b>Description</b>
Strike BadSpace_5550ff97	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 5550ff97d0ea06c9e504a41cf3a3a6ec.
Strike BadSpace_5605552d	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 5605552db8fd0f8bb93acb4ded0d1dea.
Strike BadSpace_59b7b8d2	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 59b7b8d29252a9128536fdbd08d24375f.
Strike BadSpace_59fcd8a5	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 59fcd8a54f43d911fc7a8945e07b0246.
Strike BadSpace_5adb21fd	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 5adb21fdd3dab0d714020460b7acbc4.
Strike BadSpace_5b0d48ac	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 5b0d48acc06b1091a08cd3d98516eba2.

<b>Name</b>	<b>Description</b>
Strike BadSpace_5dbe8d44	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 5dbe8d44777587e3f0655b7114775806.
Strike BadSpace_5fa10a64	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 5fa10a64b7e1fcfc3d8b8d45cefb6f837.
Strike BadSpace_5ffe6c9e	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 5ffe6c9e96924ec2fb32fd824ccc712f.
Strike BadSpace_602c84c1	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 602c84c160f4347f8adfb4a51fb0df16.
Strike BadSpace_61dcce14	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 61dcce148b5397704bcea94e54a4a67c.
Strike BadSpace_63dc5c87	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 63dc5c870ef31ee701ad346c511e213e.

<b>Name</b>	<b>Description</b>
Strike BadSpace_64a7b2f2	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 64a7b2f22e49a658370c8fc217cdcf2b.
Strike BadSpace_6867a9a1	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 6867a9a1edb61603c60649d8a09a3421.
Strike BadSpace_689f2b33	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 689f2b336291f7348045f3bede30b486.
Strike BadSpace_6d1b402e	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 6d1b402e19757a872a00d38809f40e3a.
Strike BadSpace_6daf01e7	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 6daf01e730be4ae2abbfa8bc789387e5.
Strike BadSpace_71de53b4	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 71de53b41204cbf6ec453257897f4e0c.

<b>Name</b>	<b>Description</b>
Strike BadSpace_72245569	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 722455694f18b088a3829127d3c29d67.
Strike BadSpace_7227ed73	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 7227ed73b3487c11404ec0fdde39a3be.
Strike BadSpace_750984a2	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 750984a2b401185986ff4312556f401f.
Strike BadSpace_770adcaf	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 770adcafeb4a25717460378e6786a077.
Strike BadSpace_7a799f4f	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 7a799f4f9aa63745a75b901a392aff29.
Strike BadSpace_817553a7	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 817553a753d57fcf225ccc8b1e9dcdf3.

<b>Name</b>	<b>Description</b>
Strike BadSpace_837f7071	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 837f707140e6a97b30c4284013f4ff19.
Strike BadSpace_889bfaf8	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 889bfaf82833015fe6cb81d50d4a8b70.
Strike BadSpace_88ba6eb4	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 88ba6eb42ccf6af12bf06caf3719bd98.
Strike BadSpace_88ebad86	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 88ebad865a68a0eb5a67e2394d42568d.
Strike BadSpace_8ba956a3	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 8ba956a3ef249ee32236956631353433.
Strike BadSpace_8bd43117	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 8bd43117753127bd3e720676ae28487f.

<b>Name</b>	<b>Description</b>
Strike BadSpace_8d35c719	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 8d35c719eec61e6460ed333e49a82f43.
Strike BadSpace_93c2c17a	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 93c2c17a62d622cc62b74576e876d297.
Strike BadSpace_96837e4f	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 96837e4f3349f1b980b1a08edece9139.
Strike BadSpace_9858470c	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 9858470c32fb5b76a744b55846745238.
Strike BadSpace_9881f581	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 9881f5811d056f901f1bdd43be0b1f21.
Strike BadSpace_98d2b07d	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 98d2b07dcf3ab7f6b21d8a1c45140006.

<b>Name</b>	<b>Description</b>
Strike BadSpace_9b3f750c	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 9b3f750c0cd0a04bb7a78525d174f6e6.
Strike BadSpace_9cb0aca5	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 9cb0aca5d284fc27b32104741e8c114b.
Strike BadSpace_9d0ea20d	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 9d0ea20dcdd80570e1d6bd51bd1279f7.
Strike BadSpace_9e0edd34	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 9e0edd34efbde29db56908c6d61f5f7b.
Strike BadSpace_9e993a7f	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 9e993a7fd1efe5bb0fcb58917ae984d0.
Strike BadSpace_9f18b5cb	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is 9f18b5cb4e1839beb7931fd8c3cfb191.

<b>Name</b>	<b>Description</b>
Strike BadSpace_a264caa9	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is a264caa9e5b6763590d89f1e72fb8c0c.
Strike BadSpace_a4025e15	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is a4025e15bd21b67e0f6fe334ffba8a6e.
Strike BadSpace_a47ea347	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is a47ea3473bd258d4c24ef24a59ee2ad8.
Strike BadSpace_a5f4ff64	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is a5f4ff6471cc3268bcfa8473e6b131c3.
Strike BadSpace_a65d4764	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is a65d4764e33de3755ec8bde3e8a0af1f.
Strike BadSpace_a858dbf0	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is a858dbf0202653af6e31fa01f110bef9.

<b>Name</b>	<b>Description</b>
Strike BadSpace_ae08ff4c	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is ae08ff4c3b9b6eeba0c4e954c2066e62.
Strike BadSpace_ae177463	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is ae1774635db4dc36f2e827a120d50d04.
Strike BadSpace_af2f92f5	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is af2f92f570434753867410a7931d69f8.
Strike BadSpace_b053fd87	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is b053fd879d964b3c76e60732b81bb0af.
Strike BadSpace_b1d44681	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is b1d446811b9484bb907092b5bbc06658.
Strike BadSpace_ba297df7	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is ba297df7a34468cbd04874dbb9a9ff6a.

<b>Name</b>	<b>Description</b>
Strike BadSpace_bb0dc0a3	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is bb0dc0a32d05cfdcc59e60aa640cbcee.
Strike BadSpace_bcebec5b	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is bcebec5bf8e25f8a7ec9bd5887345d24.
Strike BadSpace_bd8bf63b	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is bd8bf63bddfd91b8b6cc9dfed587b7d1.
Strike BadSpace_bf7f711e	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is bf7f711e823916e5f56ff4d2286ee866.
Strike BadSpace_c0d7b468	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is c0d7b4686ba1ce422acf8f1059363229.
Strike BadSpace_c16bdc61	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is c16bdc61bbc82e9668f8cee9cc5c94c5.

<b>Name</b>	<b>Description</b>
Strike BadSpace_c2946867	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is c2946867df12646636a1668dce52a5e8.
Strike BadSpace_c787cc5c	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is c787cc5c8c04ea691cf6fa8ae36a8308.
Strike BadSpace_c8d3708c	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is c8d3708c2801c179434a663196ff0376.
Strike BadSpace_ca232024	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is ca2320248f1c1f0935510e462bec81f2.
Strike BadSpace_cbaf38da	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is cbaf38da2653183cee6bcf29d2c4697b.
Strike BadSpace_cf01b85e	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is cf01b85e76f6aa1a7570664407ae61d3.

<b>Name</b>	<b>Description</b>
Strike BadSpace_d7babbf4	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is d7babbf43c97f6c012058267be5c2835.
Strike BadSpace_d9b3ff85	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is d9b3ff853c9d28392b0c869ea8c1729c.
Strike BadSpace_d9cf0fb3	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is d9cf0fb39a67e4a1163c172863eb4fa9.
Strike BadSpace_dddececa	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is dddececac9dacfb7fce6f7fb6fc29334.
Strike BadSpace_de0c31f5	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is de0c31f523c1c5632f2404abcaa4f6b4.
Strike BadSpace_dfbe3f12	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is dfbe3f1221933a43ba4e87bf8e70a07f.

<b>Name</b>	<b>Description</b>
Strike BadSpace_dfc08e40	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is dfc08e405abb187a4b9d120f31ab6b30.
Strike BadSpace_e49e35d6	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is e49e35d6838821efed91d1c403d6e4a1.
Strike BadSpace_e4f5640c	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is e4f5640cdfcff41a7f6b23d4dd3cf9a4.
Strike BadSpace_ec534a65	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is ec534a6532a3d0bcb0aca0254baa1b94.
Strike BadSpace_edcaaeb7	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is edcaaeb77d6ea4869333902e2af61ac2.
Strike BadSpace_ef401948	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is ef401948a5d0428c328ea1454d2f92fb.

<b>Name</b>	<b>Description</b>
Strike BadSpace_efafa11c	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is efafa11c77ea43b6e06f342448295115.
Strike BadSpace_efc73651	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is efc7365134a29bbcd549aa262fcdad1c.
Strike BadSpace_f1251f37	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is f1251f37e80bc18e7d6b7e8ee2180b09.
Strike BadSpace_f2a40149	This strike sends a malware sample known as BadSpace. BadSpace is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is f2a4014997dd068bbe3eccceb482d21f.
Strike BadSpace_f3f654d3	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is f3f654d3cc395793f7f31c709b264c1c.
Strike BadSpace_f47f5f4a	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is f47f5f4a8d87b0e62f9c7104ff9a2845.

<b>Name</b>	<b>Description</b>
Strike BadSpace_f59fb887	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is f59fb887879f1f4200dc8c09539d0ef0.
Strike BadSpace_f666b72a	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is f666b72a961983c821d31f8501ee11e4.
Strike BadSpace_f71b251a	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is f71b251a4a95a6b302aa63b939f0f03d.
Strike BadSpace_fb8082d4	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is fb8082d475179b1abbac509c49d18b8e.
Strike BadSpace_fc4317b8	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is fc4317b8775ead714f76c3c9280eac57.
Strike BadSpace_fd24f4d9	This strike sends a malware sample known as BadSpace. BadSpace also known as WarmCookie is a backdoor malware that is delivered via infected websites. Once downloaded and infected the malware opens up C2 communication with a remote server using the target specific information to encrypt the data being sent. The malware supports several commands from the remote server including the ability to take a screenshot, execute commands, and read and write files. The MD5 hash of this BadSpace sample is fd24f4d9af1c2f1f997aae9ef24baf7d.

<b>Name</b>	<b>Description</b>
Strike Bandidos_038de761	This strike sends a malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The MD5 hash of this Bandidos sample is 038de761c002ae546870035be143a736.
Strike Bandidos_06d613cc	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has random bytes appended at the end of the file. The MD5 hash of this Bandidos sample is 06d613ccf59608145e0ef7235f9ff4c6.
Strike Bandidos_0f31bba7	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has random bytes appended at the end of the file. The MD5 hash of this Bandidos sample is 0f31bba7e0fe074a70230e5504ab1bc0.
Strike Bandidos_10c4865e	This strike sends a malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The MD5 hash of this Bandidos sample is 10c4865edac377dc12f14905c8bb3a46.
Strike Bandidos_2d9afda2	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Bandidos sample is 2d9afda2d563179aa8230116f916d227.

<b>Name</b>	<b>Description</b>
Strike Bandidos_3015f878	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Bandidos sample is 3015f8785e0aa11d0cc1eadfe6112916.
Strike Bandidos_4ba8ccbd	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has been packed using upx packer, with the default options. The MD5 hash of this Bandidos sample is 4ba8ccbd73a0951cab9c156fea290a70.
Strike Bandidos_4dc64170	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Bandidos sample is 4dc6417077e498a189e40dde2efd41da.
Strike Bandidos_64acb89a	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Bandidos sample is 64acb89ad84db2d5f2bad354ad547417.
Strike Bandidos_695ebe3e	This strike sends a malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The MD5 hash of this Bandidos sample is 695ebe3e45a89552d7dabbc2b972ed66.

<b>Name</b>	<b>Description</b>
Strike Bandidos_78cb7d1e	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Bandidos sample is 78cb7d1e62e3340825e8db41e752bdb8.
Strike Bandidos_808ffbe3	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Bandidos sample is 808ffbe38c037d877279779ea356e0a4.
Strike Bandidos_80bda1f2	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Bandidos sample is 80bda1f2647c16ed8050162359401c28.
Strike Bandidos_86657996	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Bandidos sample is 866579961556526d991a5917a5adc665.
Strike Bandidos_998462a8	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Bandidos sample is 998462a846d496b57b30b5f39ee118b0.

<b>Name</b>	<b>Description</b>
Strike Bandidos_a09d7cb6	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Bandidos sample is a09d7cb6933ebc776f1321b9e41599a6.
Strike Bandidos_b89e1cb9	This strike sends a malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the PDF. The MD5 hash of this Bandidos sample is b89e1cb9522fbf1a4b54450b0c0c8781.
Strike Bandidos_bb861561	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has random bytes appended at the end of the file. The MD5 hash of this Bandidos sample is bb8615619a3363acd508ca02384c1ead.
Strike Bandidos_c1a93313	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has the checksum removed in the PE file format. The MD5 hash of this Bandidos sample is c1a933139452f8672e4810333a3d43db.
Strike Bandidos_eb5f7076	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Bandidos sample is eb5f7076a810e1dcd7797545f05e5664.

<b>Name</b>	<b>Description</b>
Strike Bandidos_fc89c12d	This strike sends a polymorphic malware sample known as Bandidos. Recently this campaign was largely found targeting Venezuela and Spanish speaking countries. Infection occurs when malicious emails are sent with a PDF document to their victims. Once the PDF is opened and the link clicked an archive is retrieved with a dropper that injects Bandook into Internet Explorer. The Bandidos payload has many features including manipulating files, taking screenshots, controlling the user cursor on screen, installing additional DLLs, uninstalling itself, and exfiltrating data. This sample is the Dropper. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Bandidos sample is fc89c12d2438bf86a0983305e9b76ff4.
Strike Banload_03dd8ecd	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 03dd8ecd823550d572e3cd6a1d8affda.
Strike Banload_0658bb95	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 0658bb95e633fdb10f56edabc5d3fa8a.
Strike Banload_06d7088e	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 06d7088ee3d6560a888025a8c28cabef0.
Strike Banload_07816243	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 0781624361d6a6f65cd2c114ec4d800a.
Strike Banload_08b7011c	This strike sends a polymorphic malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Banload sample is 08b7011cafef2b3617b2c7a6eac91d51.
Strike Banload_098f304b	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 098f304b725e0c4139056cc20c7418e5.
Strike Banload_0bdc9790	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 0bdc979054ee50b70c462b2a3ad8bcb6.
Strike Banload_17da0ba7	This strike sends a polymorphic malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Banload sample is 17da0ba7634ca9018ee19c56cb725985.

<b>Name</b>	<b>Description</b>
Strike Banload_19b2502d	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 19b2502d914c566558be34907e3d6cc8.
Strike Banload_1efa5710	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 1efa5710fcab7a4f37edb10a305a8565.
Strike Banload_1f9222f2	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 1f9222f29c3e53289a9242bb7aac87e2.
Strike Banload_21f7c59c	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 21f7c59c14c55dabd0b9dc42b2a13e65.
Strike Banload_23c1d4e3	This strike sends a polymorphic malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The binary has been packed using upx packer, with the default options. The MD5 hash of this Banload sample is 23c1d4e3c2d7f46928ac7e09b19534df.
Strike Banload_27fbaf16	This strike sends a polymorphic malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The binary has random bytes appended at the end of the file. The MD5 hash of this Banload sample is 27fbaf16b606687ee8e9e5a42c47ff4e.
Strike Banload_31b3d6d4	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 31b3d6d42570a7e46c9a49fc352496d4.
Strike Banload_3c8d18b6	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 3c8d18b6e55095a225e09bbe7a171fc4.
Strike Banload_48527475	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 485274755aecfc2f3c577eb6aa61cc4.
Strike Banload_49c1c132	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 49c1c1326133f028e89bded056d32b9c.

<b>Name</b>	<b>Description</b>
Strike Banload_54ba4069	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 54ba40694472ffb6b9ae416c9c48ba4d.
Strike Banload_57890324	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 5789032400a88264ddd37c1599304bd2.
Strike Banload_5e5b471d	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 5e5b471dde3fa11cce485958858f6419.
Strike Banload_5f4c32fd	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 5f4c32fdc71c7d660158b4a4e5f0cc73.
Strike Banload_62d4cbbe	This strike sends a polymorphic malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Banload sample is 62d4cbbee0dacd83933816350ff340e7.
Strike Banload_64cada78	This strike sends a polymorphic malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The binary has the checksum removed in the PE file format. The MD5 hash of this Banload sample is 64cada78fb8d2be8321c64030fb06347.
Strike Banload_66b8cd3b	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 66b8cd3b1eb25169bf41beba0fc5c788.
Strike Banload_6c2ad02c	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 6c2ad02c4757738a272804d6d9bea945.
Strike Banload_6c65c7e6	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 6c65c7e6a017df322ef5f3f5746b933a.
Strike Banload_6d1bdafed	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 6d1bdafed059c665ed9abca1c5f55767.

<b>Name</b>	<b>Description</b>
Strike Banload_793d4b0e	This strike sends a polymorphic malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Banload sample is 793d4b0ed7b759650ca4a7aeceff56c9.
Strike Banload_7a804fc3	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 7a804fc38cac8743b3484a3faf74a33b.
Strike Banload_7c5d1fa0	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 7c5d1fa04c00c879d314027f037e0abf.
Strike Banload_7f5fd9a3	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 7f5fd9a3772ca1d9e2e4ad11132d89a4.
Strike Banload_7fa2373e	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 7fa2373eb569259cda8c858bbd553e6d.
Strike Banload_80cb5601	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 80cb5601683bbc10eaa9bd6c0a69ff29.
Strike Banload_812ad9e9	This strike sends a polymorphic malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The binary has been packed using upx packer, with the default options. The MD5 hash of this Banload sample is 812ad9e973bb20f736f9455578785570.
Strike Banload_817f6461	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 817f6461ce3b8252058920db2cfc9942.
Strike Banload_8bbc6745	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 8bbc6745481a14d26d118c7a36dbe57d.
Strike Banload_8c79f698	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 8c79f698f784995d572bbe1259d62b4e.

<b>Name</b>	<b>Description</b>
Strike Banload_94a170cb	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 94a170cb5beb4d608e23d55533c86ee.
Strike Banload_95dd67c2	This strike sends a polymorphic malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Banload sample is 95dd67c228fe6339411c6809cebfbb96.
Strike Banload_9769f7da	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 9769f7dae9a2ae1d6ec10cbdbbb2ee2c.
Strike Banload_9f95f5e6	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is 9f95f5e64e39f57da72e25d609f64586.
Strike Banload_a2a81870	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is a2a81870c33b35d6cd0092e992f1b4c4.
Strike Banload_aa0220fc	This strike sends a polymorphic malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Banload sample is aa0220fc966bd466016cb8d43aa157e9.
Strike Banload_ab0d89d2	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is ab0d89d2a3aae61867d2f74734247be4.
Strike Banload_b0f6797f	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is b0f6797f35d9b0845d0208b5ee2b2d95.
Strike Banload_b49b6484	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is b49b64848bec6f371a87bb3299289fe6.
Strike Banload_b942612e	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is b942612eebef0bf2cc17e649da42f645.

<b>Name</b>	<b>Description</b>
Strike Banload_c2076b76	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is c2076b766832250f6a662167587ff22f.
Strike Banload_c4d27160	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is c4d27160fcce47b741bb2dad01d63b20.
Strike Banload_c6780923	This strike sends a polymorphic malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The binary has the checksum removed in the PE file format. The MD5 hash of this Banload sample is c6780923def330192f69eb7826249c62.
Strike Banload_c8181d11	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is c8181d11545ed27d3942832216d2baa8.
Strike Banload_d93d32b2	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is d93d32b2df1365aba50a850cdcf9ac41.
Strike Banload_dc2c2460	This strike sends a polymorphic malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Banload sample is dc2c2460f88c67ba4596bdfb34b2cbac.
Strike Banload_deaf3862	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is deaf38621cc351ca073766c3217631d0.
Strike Banload_e3117df8	This strike sends a polymorphic malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Banload sample is e3117df8ed16e72bf66ef6b10e5e9b02.
Strike Banload_f9295e9d	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is f9295e9d59544554999c80a0be5ea322.
Strike Banload_f9606989	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is f9606989388e71a12e1fb6e0ee1b7210.

<b>Name</b>	<b>Description</b>
Strike Banload_fa2ac90f	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is fa2ac90fe8bbfa7a11b40f18bf21045c.
Strike Banload_fbed3502	This strike sends a malware sample known as Banload. Banload is a banking trojan that has recently been infecting Latin American systems. This malware uses custom kernel drivers to evade detection. The MD5 hash of this Banload sample is fbed3502397bc90ac4008f6593c666a6.
Strike Barys_006a7221	This strike sends a malware sample known as Barys. Barys is a trojan and downloader that will upload malicious files to the victim machine. The MD5 hash of this Barys sample is 006a72219afabff2f56695f413ca43db.
Strike Barys_1aeb9636	This strike sends a malware sample known as Barys. Barys is a trojan and downloader that will upload malicious files to the victim machine. The MD5 hash of this Barys sample is 1aeb9636011a15736fa535f7d3ba7f9d.
Strike Barys_20d6e9bb	This strike sends a malware sample known as Barys. Barys is a trojan and downloader that will upload malicious files to the victim machine. The MD5 hash of this Barys sample is 20d6e9bb4eb08715b9c14437b90c059d.
Strike Barys_2775ccd0	This strike sends a polymorphic malware sample known as Barys. Barys is a trojan and downloader that will upload malicious files to the victim machine. The binary has a new section added in the PE file format with random contents. The MD5 hash of this Barys sample is 2775ccd010831c057c8d3c822adf7fc3.
Strike Barys_2f511a1d	This strike sends a polymorphic malware sample known as Barys. Barys is a trojan and downloader that will upload malicious files to the victim machine. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Barys sample is 2f511a1df6582dea8340fd62e27c9f3e.
Strike Barys_36642d69	This strike sends a malware sample known as Barys. Barys is a trojan and downloader that will upload malicious files to the victim machine. The MD5 hash of this Barys sample is 36642d69e2d734c634e8fa854e54ecae.
Strike Barys_3c11a2bd	This strike sends a polymorphic malware sample known as Barys. Barys is a trojan and downloader that will upload malicious files to the victim machine. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Barys sample is 3c11a2bd2d5f1c68588dd60b742008f1.
Strike Barys_6a191144	This strike sends a polymorphic malware sample known as Barys. Barys is a trojan and downloader that will upload malicious files to the victim machine. The binary has random bytes appended at the end of the file. The MD5 hash of this Barys sample is 6a191144dc2744c0d803461b8b35336b.
Strike Barys_c594feb4	This strike sends a polymorphic malware sample known as Barys. Barys is a trojan and downloader that will upload malicious files to the victim machine. The binary has random bytes appended at the end of the file. The MD5 hash of this Barys sample is c594feb41863cd0726eadf0e1c376ee6.

<b>Name</b>	<b>Description</b>
Strike Barys_d1365296	This strike sends a polymorphic malware sample known as Barys. Barys is a trojan and downloader that will upload malicious files to the victim machine. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Barys sample is d1365296a329a50b6d389373aa50fa01.
Strike Barys_f7298f17	This strike sends a malware sample known as Barys. Barys is a trojan and downloader that will upload malicious files to the victim machine. The MD5 hash of this Barys sample is f7298f1722540763da5a2e2c82368b25.
Strike Barys_f815281e	This strike sends a malware sample known as Barys. Barys is a trojan and downloader that will upload malicious files to the victim machine. The MD5 hash of this Barys sample is f815281ed4b16169e0b474dbac612bbc.
Strike BazaLoader_034e2d69	This strike sends a polymorphic malware sample known as BazaLoader. BazaLoader is a modular malware loader with the purpose to deliver additional malware. Most recently BazaLoader campaigns have been detected delivering email and document lures related to Valentine's Day. The binary file has one more imports added in the import table. The MD5 hash of this BazaLoader sample is 034e2d6983dfcd827b99f8592aba6acf.
Strike BazaLoader_3c9d6dd0	This strike sends a polymorphic malware sample known as BazaLoader. BazaLoader is a modular malware loader with the purpose to deliver additional malware. Most recently BazaLoader campaigns have been detected delivering email and document lures related to Valentine's Day. The binary has the timestamp field updated in the PE file header. The MD5 hash of this BazaLoader sample is 3c9d6dd012f71a9d021227ef35c593d4.
Strike BazaLoader_50a737ac	This strike sends a malware sample known as BazaLoader. BazaLoader is a modular malware loader with the purpose to deliver additional malware. Most recently BazaLoader campaigns have been detected delivering email and document lures related to Valentine's Day. The MD5 hash of this BazaLoader sample is 50a737acebc342a7d5bdca05419c1564.
Strike BazaLoader_66a795a6	This strike sends a polymorphic malware sample known as BazaLoader. BazaLoader is a modular malware loader with the purpose to deliver additional malware. Most recently BazaLoader campaigns have been detected delivering email and document lures related to Valentine's Day. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this BazaLoader sample is 66a795a6c30b329d358293a47ad02de5.
Strike BazaLoader_8ef02674	This strike sends a polymorphic malware sample known as BazaLoader. BazaLoader is a modular malware loader with the purpose to deliver additional malware. Most recently BazaLoader campaigns have been detected delivering email and document lures related to Valentine's Day. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this BazaLoader sample is 8ef02674c322336d04f054f470eea0ce.
Strike BazarLoader_1d528a2e	This strike sends a malware sample known as BazarLoader. BazarLoader is a malware loader with the function to install and download additional malware. This sample of BazarLoader is Nim-compiled to make detection more difficult. The MD5 hash of this BazarLoader sample is 1d528a2e1d0a097421e57f86ba04e79f.

<b>Name</b>	<b>Description</b>
Strike BazarLoader_4faef841	This strike sends a malware sample known as BazarLoader. BazarLoader is a malware loader with the function to install and download additional malware like Trickbot or Ryuk. The MD5 hash of this BazarLoader sample is 4faef8417a45888b6a1b8ddadd4332c8.
Strike BazarLoader_6b77b33b	This strike sends a malware sample known as BazarLoader. BazarLoader is a malware loader with the function to install and download additional malware like Trickbot or Ryuk. The MD5 hash of this BazarLoader sample is 6b77b33b880eda3a3527d489fb213d97.
Strike BazarLoader_a8e44d19	This strike sends a malware sample known as BazarLoader. BazarLoader is a malware loader with the function to install and download additional malware like Trickbot or Ryuk. The MD5 hash of this BazarLoader sample is a8e44d190da9ca504c12f576fa9a417a.
Strike BazarLoader_aedbdc94	This strike sends a malware sample known as BazarLoader. BazarLoader is a malware loader with the function to install and download additional malware like Trickbot or Ryuk. The MD5 hash of this BazarLoader sample is aedbdc94d6c5cf73533f71ea8b5f5eea.
Strike BazarLoader_f6da98fd	This strike sends a malware sample known as BazarLoader. BazarLoader is a malware loader with the function to install and download additional malware like Trickbot or Ryuk. The MD5 hash of this BazarLoader sample is f6da98fd1bbbf7e2c0c5ef0718380e61.
Strike BeaverTail_19fed025	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is 19fed025bf280190948a4c14a9ff8786.
Strike BeaverTail_4b5fdb56	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is 4b5fdb56a090de9ff532764c3f817183.
Strike BeaverTail_4eaefb2f	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is 4eaefb2fc78df5118aa943301b57391b.

<b>Name</b>	<b>Description</b>
Strike BeaverTail_55430683	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is 554306835785d730a6bddbc68e12d3f0.
Strike BeaverTail_564a7352	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is 564a73529560821b21fe576ee642dd70.
Strike BeaverTail_5f6a62a0	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is 5f6a62a09c0f5dce9d99740d5d1a52b8.
Strike BeaverTail_6c36176f	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is 6c36176f8ae04c27574fa6670e41301c.
Strike BeaverTail_8b3c5fa4	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is 8b3c5fa4d1ef167b13716d5062f26c27.

<b>Name</b>	<b>Description</b>
Strike BeaverTail_93f4ab5b	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is 93f4ab5b5611f7388a8c6c27f28487e5.
Strike BeaverTail_b70d6184	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is b70d6184796e5d62ea40e6dc08c22d3e.
Strike BeaverTail_bf7c42a9	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is bf7c42a9d8dc2dcefbc3f0d0d3698c.
Strike BeaverTail_c0164d2e	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is c0164d2eb0494a4879f67f3b90ed3ae3.
Strike BeaverTail_c8dbcacf	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is c8dbcacf2c4462b0465dda855db1f1fe.

<b>Name</b>	<b>Description</b>
Strike BeaverTail_e8983ea8	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is e8983ea817241e4ce8684263b9409f58.
Strike BeaverTail_ef9a40f9	This strike sends a malware sample known as BeaverTail. BeaverTail is a JavaScript-based malware distributed through Node Package Manager (NPM) packages. The malware serves as an information stealer targeting cryptocurrency wallets and credit card details. It also acts as a loader for the subsequent malware, InvisibleFerret. It is heavily obfuscated and often injected into legitimate NPM projects and requires human interaction for execution, contributing to its evasion tactics. Once installed on any cross-platform it collects system information and searches for browser extensions associated with cryptocurrency wallets. The MD5 hash of this BeaverTail sample is ef9a40f9c8c1355340bd83f6a5a36d93.
Strike Bellingcat_b4f10039	This strike sends a malware sample known as Bellingcat. The malware sample belongs to a Russian APT group that uses spear-phishing messages to target specific entities. The attack uses a NASA-themed tactic, which delivers a ZIP file containing an LNK file disguised as a PDF. The LNK file executes a PowerShell script to decode and execute a Base64-encoded command, deploying the HTTP-Shell multi-platform reverse shell. The shell is capable of file upload/download and C&C communication, aimed to mimic legitimate activity for stealth. The MD5 hash of this Bellingcat sample is b4f10039927b040f0470b956c74a31b4.
Strike Bellingcat_b58d686f	This strike sends a malware sample known as Bellingcat. The malware sample belongs to a Russian APT group that uses spear-phishing messages to target specific entities. The attack uses a NASA-themed tactic, which delivers a ZIP file containing an LNK file disguised as a PDF. The LNK file executes a PowerShell script to decode and execute a Base64-encoded command, deploying the HTTP-Shell multi-platform reverse shell. The shell is capable of file upload/download and C&C communication, aimed to mimic legitimate activity for stealth. The MD5 hash of this Bellingcat sample is b58d686f1c6c124ccd8d5fab08638ec8.
Strike Bellingcat_bf8a44df	This strike sends a malware sample known as Bellingcat. The malware sample belongs to a Russian APT group that uses spear-phishing messages to target specific entities. The attack uses a NASA-themed tactic, which delivers a ZIP file containing an LNK file disguised as a PDF. The LNK file executes a PowerShell script to decode and execute a Base64-encoded command, deploying the HTTP-Shell multi-platform reverse shell. The shell is capable of file upload/download and C&C communication, aimed to mimic legitimate activity for stealth. The MD5 hash of this Bellingcat sample is bf8a44df0ea8e72cf03237e166f414a7.

<b>Name</b>	<b>Description</b>
Strike Bellingcat_eaec51e0	This strike sends a malware sample known as Bellingcat. The malware sample belongs to a Russian APT group that uses spear-phishing messages to target specific entities. The attack uses a NASA-themed tactic, which delivers a ZIP file containing an LNK file disguised as a PDF. The LNK file executes a PowerShell script to decode and execute a Base64-encoded command, deploying the HTTP-Shell multi-platform reverse shell. The shell is capable of file upload/download and C&C communication, aimed to mimic legitimate activity for stealth. The MD5 hash of this Bellingcat sample is eaec51e070790ef819e7837b880acf0a.
Strike Bellingcat_f2bc317c	This strike sends a malware sample known as Bellingcat. The malware sample belongs to a Russian APT group that uses spear-phishing messages to target specific entities. The attack uses a NASA-themed tactic, which delivers a ZIP file containing an LNK file disguised as a PDF. The LNK file executes a PowerShell script to decode and execute a Base64-encoded command, deploying the HTTP-Shell multi-platform reverse shell. The shell is capable of file upload/download and C&C communication, aimed to mimic legitimate activity for stealth. The MD5 hash of this Bellingcat sample is f2bc317ce04727cc99cfb6225e2a2802.
Strike Bifrost_025d7085	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 025d7085a1091019ca20a9765c0aaeb8.
Strike Bifrost_04e53cad	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 04e53cad12c002afe77882e0b1d6ce6a.
Strike Bifrost_0d1327d2	This strike sends a polymorphic malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Bifrost sample is 0d1327d2a2b0a068192d16b5b75b9e10.
Strike Bifrost_11ac73b0	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 11ac73b0ffdf22b9b329bfddf215ed83.
Strike Bifrost_1208f352	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 1208f3526e1cd37fa37017c07bda23e9.

<b>Name</b>	<b>Description</b>
Strike Bifrost_1216aa41	This strike sends a polymorphic malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Bifrost sample is 1216aa4137de1ab5dd6941072e4dfbb7.
Strike Bifrost_175db028	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 175db028ffcd0b6c109d80b3d9cfa06f.
Strike Bifrost_188de6b9	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 188de6b94cd471e27fb24bae4ffddef1.
Strike Bifrost_19f419d8	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 19f419d85734514f263386cb75a3fd23.
Strike Bifrost_1acfcede	This strike sends a polymorphic malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Bifrost sample is 1acfcede2b9e9d76d699f401e2c7ffe2.
Strike Bifrost_2660414d	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 2660414d630a3c751741356fc39e6976.
Strike Bifrost_28c3852d	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 28c3852dadec6b0a094560110dff9d90.
Strike Bifrost_2b7726fa	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 2b7726fa3e1695bce3a95d8222ebaf07.

<b>Name</b>	<b>Description</b>
Strike Bifrost_2bcd1b5	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 2bcd1b533f88165e5ef0da754517536.
Strike Bifrost_2d909a3d	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 2d909a3d5efa68b5d8b2553db1c13e7f.
Strike Bifrost_2f0c11af	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 2f0c11af00219f9eec567c45a1ae97ff.
Strike Bifrost_313e9588	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 313e958863a7e7577a6c677c17d4ddff.
Strike Bifrost_31d773b4	This strike sends a polymorphic malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Bifrost sample is 31d773b42bd89af8689182e72170cbf4.
Strike Bifrost_3782d221	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 3782d2215918964a26919546a73600fe.
Strike Bifrost_37c49bbd	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 37c49bbd0788943d753638da6ee74b69.
Strike Bifrost_399c3a89	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 399c3a89a43ab12f22d0218a717355ec.

<b>Name</b>	<b>Description</b>
Strike Bifrost_3f548dd8	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 3f548dd8eeb144a6f0d35277083b5b39.
Strike Bifrost_401423b3	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 401423b33f7e755449450a2badb533be.
Strike Bifrost_414a5427	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 414a5427b5d510b7f1eaf3c79c95e591.
Strike Bifrost_4294edbd	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 4294edbd3d7041c08ca4af8dbec9b83f.
Strike Bifrost_442093d3	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 442093d33f762e6a42d1cf33087693e6.
Strike Bifrost_4511d282	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 4511d282ddf3d91fca9e3882e1cba606.
Strike Bifrost_4b0ed0b3	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 4b0ed0b302fb3388e431a3e6809d3556.
Strike Bifrost_4b22d70c	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 4b22d70c0ebd8f3900e9ac41144833c2.
Strike Bifrost_4c39d9a1	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 4c39d9a16e07a866fd6b34604cd32860.

<b>Name</b>	<b>Description</b>
Strike Bifrost_4f1975b3	This strike sends a polymorphic malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The binary has random bytes appended at the end of the file. The MD5 hash of this Bifrost sample is 4f1975b3411e631aa3340b0b278c6aff.
Strike Bifrost_4f86b517	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 4f86b517e0ff6130ae58d272476f5de8.
Strike Bifrost_4ff40064	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 4ff400648d164083a47963675b66d959.
Strike Bifrost_50c35460	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 50c35460a0eb4151aee2ad125710ee03.
Strike Bifrost_51d44d8f	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 51d44d8fcdd031a645e823d282e7d047.
Strike Bifrost_54170d06	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 54170d062684ad47af4fc1e9ee8213fe.
Strike Bifrost_546515e5	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 546515e5184e713641dd3cebee3c89b5.
Strike Bifrost_5797bcc3	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 5797bcc39cdc4731ceae5c87a9c673f1.

<b>Name</b>	<b>Description</b>
Strike Bifrost_597907c7	This strike sends a polymorphic malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The Parent binary was packed using upx, hence this binary is the unpacked version generated using upx -d. The MD5 hash of this Bifrost sample is 597907c703cddcff731ac25dc8a8becc.
Strike Bifrost_5a40d3ac	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 5a40d3ac2a6fe1eab16d1500ede4db8c.
Strike Bifrost_5dc995dd	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 5dc995dd9da3dcfa9bd7773e07a4284e.
Strike Bifrost_5f0e5fcf	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 5f0e5fcf4039b92c816086ba6d0a7e70.
Strike Bifrost_6255dd50	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 6255dd507eaa7098a14fb139562cb060.
Strike Bifrost_6815b438	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 6815b438ef2c105a05bd5a3137da5b6c.
Strike Bifrost_6a5543ec	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 6a5543ecb7d729b1ae8859c54b1f8cb6.
Strike Bifrost_70c04126	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 70c04126abb95a5378868c486b91c453.

<b>Name</b>	<b>Description</b>
Strike Bifrost_70fa85a1	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 70fa85a168782ac467530d7d3dbf5cda.
Strike Bifrost_72f8e14e	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 72f8e14ee194325d3390fa9d558b8349.
Strike Bifrost_75648244	This strike sends a polymorphic malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Bifrost sample is 756482447e93fb7e95df47c9054308ac.
Strike Bifrost_768d0741	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 768d0741724fd868b4fee7df162482ac.
Strike Bifrost_796e5e8b	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 796e5e8b154e8defa316ada29f9c6d4c.
Strike Bifrost_7ade2faa	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 7ade2faad28324ad407b1e430fc0d4fd.
Strike Bifrost_7b2cfdf1	This strike sends a polymorphic malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Bifrost sample is 7b2cfdf149b30ce6f15c3771f77c7430.
Strike Bifrost_7bfd93ce	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 7bfd93ce9a580270c34f0ee1d96720de.

<b>Name</b>	<b>Description</b>
Strike Bifrost_84932775	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 84932775991cc72e5e11f92dd8556fd6.
Strike Bifrost_84a4df6d	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 84a4df6dc8f2ba569351868e511a8118.
Strike Bifrost_8799cf57	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 8799cf572264225b73066d118e6de76f.
Strike Bifrost_88918aa9	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 88918aa93a7020accbf4cd82147f2d1d.
Strike Bifrost_8b220453	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 8b220453ce856f3709cd80beaae503b2.
Strike Bifrost_90005a6e	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 90005a6ee45152b570fd53742b878be7.
Strike Bifrost_970f9911	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 970f9911e2c475db87a15d1c4ebdaaef.
Strike Bifrost_9d901907	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is 9d901907a3c2735f7ffd4423b2b1f065.
Strike Bifrost_a40f1e19	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is a40f1e1925d182a079015e9b8b592fdb.

<b>Name</b>	<b>Description</b>
Strike Bifrost_a6ea548d	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is a6ea548d6c680bf5e3400369361400ed.
Strike Bifrost_a890f600	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is a890f60074d5a6f3ed85182b6f25f93a.
Strike Bifrost_abdcebab	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is abdccebabc0c8ce3ddc1f1d4f11902b.
Strike Bifrost_b3a67a87	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is b3a67a8740fa1bb3627aaefdd273d18d.
Strike Bifrost_b60f966a	This strike sends a polymorphic malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Bifrost sample is b60f966ae955ef8523dd28fdb5d252c0.
Strike Bifrost_b9d3c518	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is b9d3c5182f8dca8fb5006ca1f4e5f96e.
Strike Bifrost_ba292092	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is ba29209232395b99f8792f1f0451fe28.
Strike Bifrost_bb1b81ea	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is bb1b81eae69f9128d2ff6dcaf5e35c4b.

<b>Name</b>	<b>Description</b>
Strike Bifrost_bf2fd6b7	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is bf2fd6b7c36a87815ca49a0d7b1fb291.
Strike Bifrost_c6c33227	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is c6c332277d82fc026c2cad50ed41e0d2.
Strike Bifrost_c94fc1d1	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is c94fc1d14fdb11985ecb21e74a7bc59e.
Strike Bifrost_cbe88d2a	This strike sends a polymorphic malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Bifrost sample is cbe88d2aef9baba7301620c2d1949758.
Strike Bifrost_ccda89b2	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is ccda89b2dabe18acd3832754df245eee.
Strike Bifrost_ce1ac9f5	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is ce1ac9f5aba86897dec35ae27b33fd1c.
Strike Bifrost_ce832708	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is ce832708d4933212087f74c828bbaaa5.
Strike Bifrost_d4864301	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is d4864301b4ef997adb46e544ba64b158.

<b>Name</b>	<b>Description</b>
Strike Bifrost_d533aa9f	This strike sends a polymorphic malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The binary has a new section added in the PE file format with random contents. The MD5 hash of this Bifrost sample is d533aa9f1d633528df82a69bb8c515ee.
Strike Bifrost_d5f53d7e	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is d5f53d7e5d74a981d2f15f3d953b5a90.
Strike Bifrost_d6fdcae2	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is d6fdcae22ca89a5a630f37638d2ec9f7.
Strike Bifrost_d7eabba1	This strike sends a polymorphic malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Bifrost sample is d7eabba14b4326449e5231ba9cc62194.
Strike Bifrost_d9f9f3d3	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is d9f9f3d3ebf767b3219bf16b8c3e1b80.
Strike Bifrost_df74478b	This strike sends a polymorphic malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Bifrost sample is df74478b8494a2a17157a8cd0cce6158.
Strike Bifrost_eaad1617	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is eaad1617f8f84e1072d6dc43ba791af3.
Strike Bifrost_ed5c7775	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is ed5c777571ca660b7d1eaaac12db6e17.

<b>Name</b>	<b>Description</b>
Strike Bifrost_ef19d9ec	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is ef19d9ec2a52269c50210d279066638a.
Strike Bifrost_f00b851e	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is f00b851edda9aa426fdf24b9c0679e1b.
Strike Bifrost_f3695bb5	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is f3695bb57ee730b63a99285b3e58af03.
Strike Bifrost_f844c72a	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is f844c72a7248602fbe0861525cacc8e1.
Strike Bifrost_f88047ff	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is f88047ff17da1e247c68d7e2a76732db.
Strike Bifrost_fa32787c	This strike sends a polymorphic malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The binary has the checksum removed in the PE file format. The MD5 hash of this Bifrost sample is fa32787cb971f620bed716b862ac6ed0.
Strike Bifrost_fa874b33	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is fa874b334f0797b3df342966fff5567f.
Strike Bifrost_fb998438	This strike sends a malware sample known as Bifrost. Bifrost is a backdoor that allows a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. It contains standard Remote Access Trojan capabilities including taking screenshots, camera monitoring, and keylogging. The MD5 hash of this Bifrost sample is fb998438a3d3daf91488132b1c3cb2f6.
Strike Black Basta_32f17040	This strike sends a malware sample known as Black Basta. Black Basta is ransomware that was first seen in April 2022. The most recent variants have been seen targeting vm stores on ESXI machines. The MD5 hash of this Black Basta sample is 32f17040ddaf3477008d844c8eb98410.

<b>Name</b>	<b>Description</b>
Strike Black Basta_497ef477	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 497ef4779c6770e4497adf0bc71655f1.
Strike Black Basta_b648b730	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is b648b7305df49492c44a1280ec2228a0.
Strike BlackByte_eef97710	This strike sends a malware sample known as BlackByte. BlackByte is a ransomware group that employs a ransomware-as-a-service offering to malicious actors. Once infected communication with C2 servers is established. AnyDesk remote management software is installed as well as other publicly available software like 'netscanold' or 'psexec to perform lateral movement and establish persistence on the victim's machine. Once this functionality has been established the attacker demands a bitcoin ransom in order to decrypt the files on the system. The MD5 hash of this BlackByte sample is eef977108c7a7aef512532cc6e2f49cc.
Strike BlackCat_b6b9d449	This strike sends a malware sample known as BlackCat. BlackCat is ransomware written in rust. It has been tied to the BlackMatter ransomware group. The ransomware uses AES or CHACHA20 algorithms are for file encryption, and the executable is compiled specifically for the target organization. The MD5 hash of this BlackCat sample is b6b9d449c9416abf96d21b356a41a28e.
Strike BlackMatter_1019e015	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has the checksum removed in the PE file format. The MD5 hash of this BlackMatter sample is 1019e0151d6c55eeecf06443fa6197c7.
Strike BlackMatter_1060dca3	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is 1060dca3875b4c027b247807b0a46ef9.
Strike BlackMatter_1dd464cb	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is 1dd464cbb3fb6881eeef3f05b8b1fdb5.
Strike BlackMatter_3317daac	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is 3317daace715dc332622d883091cf68b.

<b>Name</b>	<b>Description</b>
Strike BlackMatter_3f9a28e8	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is 3f9a28e8c057e7ea7ccf15a4db81f362.
Strike BlackMatter_48f3e009	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this BlackMatter sample is 48f3e0096689e5b981a7494f9373c466.
Strike BlackMatter_4c146e1f	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has the debug flag removed in the PE file format. The MD5 hash of this BlackMatter sample is 4c146e1f99bbdc09ef5fcc8780b5b844.
Strike BlackMatter_50c49700	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is 50c4970003a84cab1bf2634631fe39d7.
Strike BlackMatter_598c53bf	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is 598c53bfef81e489375f09792e487f1a.
Strike BlackMatter_60f217dd	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is 60f217dd352109f05550b9473d22dc6b.
Strike BlackMatter_61d0a6a7	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has been packed using upx packer, with the default options. The MD5 hash of this BlackMatter sample is 61d0a6a753435fd8e8993473c083b872.
Strike BlackMatter_687e5999	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this BlackMatter sample is 687e599972236164dbcdb1c229d27087.

<b>Name</b>	<b>Description</b>
Strike BlackMatter_6e9a1ea0	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is 6e9a1ea049f79e227503fb5681a58d8e.
Strike BlackMatter_6fd84253	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this BlackMatter sample is 6fd842539aa3f5fd2e0474f3b48f877a.
Strike BlackMatter_720f6799	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has the checksum removed in the PE file format. The MD5 hash of this BlackMatter sample is 720f6799e6befa45cb4233b9631f4c82.
Strike BlackMatter_9200233d	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is 9200233d9b991b290c16d33a9956bea8.
Strike BlackMatter_98a3bee4	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has been packed using upx packer, with the default options. The MD5 hash of this BlackMatter sample is 98a3bee4399116289036d0224aac78d7.
Strike BlackMatter_9d047a42	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has random bytes appended at the end of the file. The MD5 hash of this BlackMatter sample is 9d047a4230a677be7daf5268a075d7e2.
Strike BlackMatter_9fa3caf8	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary file has one more imports added in the import table. The MD5 hash of this BlackMatter sample is 9fa3cafbc2f1ded8fe92007408e7625d.
Strike BlackMatter_a6237d50	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is a6237d5041d5a178c50bcad6387b405e.

<b>Name</b>	<b>Description</b>
Strike BlackMatter_ac50d0bc	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has the checksum removed in the PE file format. The MD5 hash of this BlackMatter sample is ac50d0bc460a702822ebae99a86761b5.
Strike BlackMatter_ad291818	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is ad2918181f609861ccb7bda8ebcb10e5.
Strike BlackMatter_b492d118	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has random bytes appended at the end of the file. The MD5 hash of this BlackMatter sample is b492d118edc1f091d3371012c2463e57.
Strike BlackMatter_b5c9d7c1	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this BlackMatter sample is b5c9d7c157a3fffd0cab340313f1c5ec.
Strike BlackMatter_b73ff289	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary file has one more imports added in the import table. The MD5 hash of this BlackMatter sample is b73ff289f910386f378a9b0a86b82fe9.
Strike BlackMatter_b786eef4	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is b786eef4adf086e8dbccc1c1f8d4d164.
Strike BlackMatter_ba375d06	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is ba375d0625001102fc1f2ccb6f582d91.
Strike BlackMatter_bff66be9	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this BlackMatter sample is bff66be9812f514e2ba8bd00746ef5cf.

<b>Name</b>	<b>Description</b>
Strike BlackMatter_c06b8cb2	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is c06b8cb2c5e3e282c7cc26836ce83f9b.
Strike BlackMatter_c5ef4711	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has been packed using upx packer, with the default options. The MD5 hash of this BlackMatter sample is c5ef4711b1b6303b622a8c73f4704430.
Strike BlackMatter_cd2d2003	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is cd2d2003cc0c59535a090f015ed629b7.
Strike BlackMatter_cfacfde5	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has the debug flag removed in the PE file format. The MD5 hash of this BlackMatter sample is cfacfde557d2762c0b7932b03c683b8a.
Strike BlackMatter_d0512f20	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is d0512f2063cbd79fb0f770817cc81ab3.
Strike BlackMatter_d19ab335	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is d19ab33523d0d070451213c05ed55eba.
Strike BlackMatter_da66726c	This strike sends a polymorphic malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this BlackMatter sample is da66726c18cecc87d776623fb1a26344.
Strike BlackMatter_e6b0276b	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is e6b0276bc3f541d8ff1ebb1b59c8bd29.

<b>Name</b>	<b>Description</b>
Strike BlackMatter_ec17046c	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is ec17046c66d51485a7d029acffa1599e.
Strike BlackMatter_f13669a4	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is f13669a48189b6b982ca2ec90c596d39.
Strike BlackMatter_f263c8c7	This strike sends a malware sample known as BlackMatter. BlackMatter is a Ransomware-as-a-Service or RaaS. It has followed in the footsteps of its predecessors DarkSide and REvil with a lot of the same functionality. It can elevate privileges, kill processes, and even steals the victim's details. The MD5 hash of this BlackMatter sample is f263c8c7872ff7f565fa1c6af55b97ca.
Strike BlackSnake_afa9d7c8	This strike sends a malware sample known as BlackSnake. BlackSnake is ransomware that has been created based on the source of the Chaos ransomware. BlackSnake has a clipper module that constantly monitors the user clipboard. This module shows it specifically targets Bitcoin wallet addresses to replace with the attacker wallet address. After this the ransomware performs file encryption as expected excluding hardcoded directories enumerated by the malware. The MD5 hash of this BlackSnake sample is afa9d7c88c28e9b8cca140413cfb32e4.
Strike BlackSuit_748de529	This strike sends a malware sample known as BlackSuit. This malware sample is known as BlackSuit. It drops a ransom note in each directory that contains encrypted files. This note contains a reference to its TOR chat site as well as a unique id per victim. The MD5 hash of this BlackSuit sample is 748de52961d2f182d47e88d736f6c835.
Strike BlackSuit_9656cd12	This strike sends a malware sample known as BlackSuit. This malware sample is known as BlackSuit. It drops a ransom note in each directory that contains encrypted files. This note contains a reference to its TOR chat site as well as a unique id per victim. The MD5 hash of this BlackSuit sample is 9656cd12e3a85b869ad90a0528ca026e.
Strike Black_Basta_0bf7bc20	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 0bf7bc20496143a9f028e77ab47b4698.
Strike Black_Basta_229ec577	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 229ec577744224d4d2fb2091ac253dd8.
Strike Black_Basta_267d5c31	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 267d5c3137d313ce1a86c2f255a835e6.

<b>Name</b>	<b>Description</b>
Strike Black_Basta_2a255e75	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 2a255e75f72ac142689082437a866c32.
Strike Black_Basta_2c383f6f	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 2c383f6fa25eea59fc54e5af19861fba.
Strike Black_Basta_2f90cd68	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 2f90cd68e4a92c5151c6e43902397a13.
Strike Black_Basta_3f400f30	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 3f400f30415941348af21d515a2fc6a3.
Strike Black_Basta_403dee0d	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 403dee0dd3891459b22a8a37828b66b8.
Strike Black_Basta_470c803b	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 470c803b32209fbef09af80a1b83e6f2.
Strike Black_Basta_4e8a7b03	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 4e8a7b03ff758f5c75ce992615a14fd0.
Strike Black_Basta_53fdb92	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 53fdb923b1890d29b8f29da77995938.
Strike Black_Basta_59db7bd2	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 59db7bd22d4ec503b768e6e646205c27.
Strike Black_Basta_6441d726	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 6441d7260944bc6dc5958c5c8a05d16d.

<b>Name</b>	<b>Description</b>
Strike Black_Basta_6f01787f	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 6f01787f5f644916b2dda5b4295efa4f.
Strike Black_Basta_80ab6a4d	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 80ab6a4d16c8137308dea1dc7922bd47.
Strike Black_Basta_8bae9edb	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 8bae9edb5b1035cd52ca45b23fee29d.
Strike Black_Basta_9f727c56	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is 9f727c56a415bf8ffa884ef241bbcd10.
Strike Black_Basta_a292fee8	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is a292fee8d8db83711e72c06d6f82562d.
Strike Black_Basta_b365faeb	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is b365faebaf416681b5f376c8aa4f4470.
Strike Black_Basta_bc95f228	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is bc95f228b11fa3b4e91c30d98f9fbff.
Strike Black_Basta_c115bbbd	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is c115bbbdb1a61f8c553d74802bfd78fb.
Strike Black_Basta_d1ae7511	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is d1ae751134e04bf6188aaed148409620.
Strike Black_Basta_d50a3b60	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is d50a3b60eb046c5d7bc6768bd3d7f1b9.

<b>Name</b>	<b>Description</b>
Strike Black_Basta_e52aa8e5	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is e52aa8e50c0ccf883b7ab7f0c36bb878.
Strike Black_Basta_e7d52019	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is e7d5201947829fd265a0356771fbebe63.
Strike Black_Basta_fd3631bf	This strike sends a polymorphic malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The binary has the debug flag removed in the PE file format. The MD5 hash of this Black Basta sample is fd3631bf37c87ad210bad170d67d33b9.
Strike Black_Basta_ff2f71df	This strike sends a malware sample known as Black Basta. Black Basta is a ransomware-as-a-service that was first identified in April 2022. It obtains initial access via spearphishing emails and vulnerabilities like CVE-2024-1709. The MD5 hash of this Black Basta sample is ff2f71dffeb997583fd297695de8c4ae.
Strike Blank Grabber_05ef1387	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is 05ef1387852e2f3998fb16553d398e02.
Strike Blank Grabber_1dfcac12	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is 1dfcac1261c5a8de83c9f5285efe6eac.
Strike Blank Grabber_26a8bb47	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is 26a8bb47cefbd6bab1cb10c5108f4b67.

<b>Name</b>	<b>Description</b>
Strike Blank Grabber_28144f28	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is 28144f2874cc381824c1cde06191bfb0.
Strike Blank Grabber_445021ec	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is 445021eca48d79fc2bfb5e03baa0eb85.
Strike Blank Grabber_4984513d	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is 4984513d03a78cf0654cf2efa9fd1203.
Strike Blank Grabber_683c060c	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is 683c060cccc9ee3a5dad65946c8c9a88.
Strike Blank Grabber_6f0e94c8	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is 6f0e94c80d8b9c98ea75bff456eff5a2.

<b>Name</b>	<b>Description</b>
Strike Blank Grabber_74e4afd2	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is 74e4afd27d23e9d0b2f3ba6ba37da155.
Strike Blank Grabber_7c8c2e4b	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is 7c8c2e4beb09b7ad7376d727ba307a60.
Strike Blank Grabber_84b87739	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is 84b877394dca4f09b8320c3ac9a1d4cd.
Strike Blank Grabber_8a65bce5	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is 8a65bce5874cc2255b7ed4ae73acd8d5.
Strike Blank Grabber_a17eb2d1	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is a17eb2d181dd820bc6b65bea32554213.

Name	Description
Strike Blank Grabber_b5479bf5	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is b5479bf5c97cfa81c02676bb9335ab24.
Strike Blank Grabber_c90b1dc1	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is c90b1dc196b50dbab7584a18f47341a1.
Strike Blank Grabber_cbd90c5c	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is cbd90c5c8c6e0cbbc7963141798f367f.
Strike Blank Grabber_d99f4643	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is d99f4643fa07fa48ee5c7e700b0fd033.
Strike Blank Grabber_e106ba38	This strike sends a malware sample known as Blank Grabber. Blank Grabber is an information-stealing malware distributed through phishing packages uploaded to the Python Package Index (PyPI). The malware's primary functions include stealing Discord tokens, extracting browser passwords, targeting gaming platforms such as Minecraft and Roblox, and exfiltrating data via Discord webhooks. The malware also collects system details, Wi-Fi passwords, and IP information, all while maintaining a covert presence through file manipulation and deceptive alerts. The MD5 hash of this Blank Grabber sample is e106ba386d874f9a75bb8b3b4458c501.

<b>Name</b>	<b>Description</b>
Strike BlockBlaster_2b366e71	This strike sends a malware sample known as BlockBlaster. BlockBlaster is a malware that is delivered through the game "Abstractism" available on Steam. The malware is delivered via a game update which disguises it as an item drop system. Upon execution, the malware uses the victim's hardware to mine cryptocurrency, slowing down the system performance. Key capabilities of this malware include evasion techniques, cryptocurrency mining, and potentially stealing Steam credentials. The MD5 hash of this BlockBlaster sample is 2b366e711484cb6648e02bc9d7774f3f.
Strike BlockBlaster_7aa6b31c	This strike sends a malware sample known as BlockBlaster. BlockBlaster is a malware that is delivered through the game "Abstractism" available on Steam. The malware is delivered via a game update which disguises it as an item drop system. Upon execution, the malware uses the victim's hardware to mine cryptocurrency, slowing down the system performance. Key capabilities of this malware include evasion techniques, cryptocurrency mining, and potentially stealing Steam credentials. The MD5 hash of this BlockBlaster sample is 7aa6b31c1531f57d744dc7fde5e92338.
Strike BlockBlaster_a80a3dc3	This strike sends a malware sample known as BlockBlaster. BlockBlaster is a malware that is delivered through the game "Abstractism" available on Steam. The malware is delivered via a game update which disguises it as an item drop system. Upon execution, the malware uses the victim's hardware to mine cryptocurrency, slowing down the system performance. Key capabilities of this malware include evasion techniques, cryptocurrency mining, and potentially stealing Steam credentials. The MD5 hash of this BlockBlaster sample is a80a3dc310429fd2d98228e49157f35a.
Strike BlockBlaster_d35249a3	This strike sends a malware sample known as BlockBlaster. BlockBlaster is a malware that is delivered through the game "Abstractism" available on Steam. The malware is delivered via a game update which disguises it as an item drop system. Upon execution, the malware uses the victim's hardware to mine cryptocurrency, slowing down the system performance. Key capabilities of this malware include evasion techniques, cryptocurrency mining, and potentially stealing Steam credentials. The MD5 hash of this BlockBlaster sample is d35249a3f80fdbd17f2664e3408f78e9.
Strike BlockBlaster_dd8da7ba	This strike sends a malware sample known as BlockBlaster. BlockBlaster is a malware that is delivered through the game "Abstractism" available on Steam. The malware is delivered via a game update which disguises it as an item drop system. Upon execution, the malware uses the victim's hardware to mine cryptocurrency, slowing down the system performance. Key capabilities of this malware include evasion techniques, cryptocurrency mining, and potentially stealing Steam credentials. The MD5 hash of this BlockBlaster sample is dd8da7bae76527590f171eeda5a41987.

<b>Name</b>	<b>Description</b>
Strike BlockBlaster_f240341a	This strike sends a malware sample known as BlockBlaster. BlockBlaster is a malware that is delivered through the game "Abstractism" available on Steam. The malware is delivered via a game update which disguises it as an item drop system. Upon execution, the malware uses the victim's hardware to mine cryptocurrency, slowing down the system performance. Key capabilities of this malware include evasion techniques, cryptocurrency mining, and potentially stealing Steam credentials. The MD5 hash of this BlockBlaster sample is f240341a95f7df4c154520b841d1a5e3.
Strike BotenaGo_27a4dfa1	The malware BotenaGo is written in the open-source programming language Golang. It was originally discovered in 2021, but the source code was pushed to Github in 2022 and made available to the public. This BotenaGo variant as well as many others is expected to be used in future Exploit-Kits and malware targeting routers and IoT devices, as it contains roughly 33 exploits aimed at the vulnerabilities in these devices. To communicate it uses a reverse shell and a telnet loader to create a backdoor to receive commands from its command-and-control server. The MD5 hash of this BotenaGo sample is 27a4dfa1380e3866d89c79dd8f27f6ac.
Strike BotenaGo_29cb03ed	The malware BotenaGo is written in the open-source programming language Golang. It was originally discovered in 2021, but the source code was pushed to Github in 2022 and made available to the public. This BotenaGo variant as well as many others is expected to be used in future Exploit-Kits and malware targeting routers and IoT devices, as it contains roughly 33 exploits aimed at the vulnerabilities in these devices. To communicate it uses a reverse shell and a telnet loader to create a backdoor to receive commands from its command-and-control server. The MD5 hash of this BotenaGo sample is 29cb03edd8b97afe1d3d95c0fc6fa249.
Strike BotenaGo_aa594ae6	The malware BotenaGo is written in the open-source programming language Golang. It was originally discovered in 2021, but the source code was pushed to Github in 2022 and made available to the public. This BotenaGo variant as well as many others is expected to be used in future Exploit-Kits and malware targeting routers and IoT devices, as it contains roughly 33 exploits aimed at the vulnerabilities in these devices. To communicate it uses a reverse shell and a telnet loader to create a backdoor to receive commands from its command-and-control server. The MD5 hash of this BotenaGo sample is aa594ae685122794921ee62696102718.
Strike Brunhilda_b1b5eacc	This strike sends a malware sample known as Brunhilda. Brunhilda is an Android dropper-framework that hosts malicious applications on the Google Play Store. Recently it has been distributing the Android banking malware Vultur. Both malware families are created by the same threat actor group. The MD5 hash of this Brunhilda sample is b1b5eacc4d1cd7500e930286833f1626.
Strike Buer_093ddecf	This strike sends a polymorphic malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Buer sample is 093ddecf0e75f245cb2b3a8e431cbb06.

<b>Name</b>	<b>Description</b>
Strike Buer_1292fd2e	This strike sends a polymorphic malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The binary has a new section added in the PE file format with random contents. The MD5 hash of this Buer sample is 1292fd2e94145944fc89568de433ea78.
Strike Buer_1ab2fc91	This strike sends a polymorphic malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Buer sample is 1ab2fc91ddfc486d3ec76c36a7ec5b43.
Strike Buer_1fa27c5e	This strike sends a malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The MD5 hash of this Buer sample is 1fa27c5e084887e9e3a2e232d27e10e3.
Strike Buer_25f10854	This strike sends a polymorphic malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The binary has random bytes appended at the end of the file. The MD5 hash of this Buer sample is 25f108547ce1d51064bfd9fd083c8da5.
Strike Buer_285e5729	This strike sends a malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The MD5 hash of this Buer sample is 285e57297f578e565dc814301149edbf.
Strike Buer_2c5569c4	This strike sends a polymorphic malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The binary has the debug flag removed in the PE file format. The MD5 hash of this Buer sample is 2c5569c4873195b82b2e3a602309c338.
Strike Buer_3cd5f44	This strike sends a polymorphic malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The binary has random bytes appended at the end of the file. The MD5 hash of this Buer sample is 3cd5f4471a4f9dd34ac0b61d2f295dc.

<b>Name</b>	<b>Description</b>
Strike Buer_41f095e2	This strike sends a polymorphic malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The binary has been packed using upx packer, with the default options. The MD5 hash of this Buer sample is 41f095e2a4b692820a8d70b27ed74590.
Strike Buer_693df2e2	This strike sends a malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The MD5 hash of this Buer sample is 693df2e2029ed05eb3e7cccd214fb414f.
Strike Buer_733098ca	This strike sends a polymorphic malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The binary has been packed using upx packer, with the default options. The MD5 hash of this Buer sample is 733098cad6d135345bc00f37cdca52c5.
Strike Buer_845c6f85	This strike sends a polymorphic malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Buer sample is 845c6f85f2a58dee6c49ed47ab052662.
Strike Buer_884fa51e	This strike sends a polymorphic malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Buer sample is 884fa51e7110c68b831899626e81345a.
Strike Buer_89d8c5bd	This strike sends a malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The MD5 hash of this Buer sample is 89d8c5bdcc1dbb18e7ba59e4450fd001.
Strike Buer_8c5bd634	This strike sends a polymorphic malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The binary has the checksum removed in the PE file format. The MD5 hash of this Buer sample is 8c5bd6343ee9630d246af49ca85951b0.

<b>Name</b>	<b>Description</b>
Strike Buer_9e8ca433	This strike sends a polymorphic malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Buer sample is 9e8ca4331d3d087f6ce750c2ba8ad455.
Strike Buer_a3987c9c	This strike sends a malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The MD5 hash of this Buer sample is a3987c9c0ca7b09971a34fad7684cbc1.
Strike Buer_c397c806	This strike sends a malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The MD5 hash of this Buer sample is c397c806d3c6196f368566319880df3c.
Strike Buer_cac3879e	This strike sends a malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The MD5 hash of this Buer sample is cac3879ed9dba1145f99376c2f32ebb7.
Strike Buer_d1b2c5f7	This strike sends a polymorphic malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Buer sample is d1b2c5f79f39a646bbd29f9aebbc57e9.
Strike Buer_ef9cb824	This strike sends a polymorphic malware sample known as Buer. Buer is a first stage downloader that is used to deploy other various forms of malware like ransomware to its intended victim. It is sold as a ready to go solution in underground marketplaces for parties looking for a malware that can provide modular options for delivery. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Buer sample is ef9cb8244219f4110d208229eff412d2.
Strike BugDrop_4b3c99ae	This strike sends a malware sample known as BugDrop. BugDrop is an Android malware that masquerades as a QR code scanner on the Google Play store. Its sole purpose is to bypass security measures used in the Google Play Store, and deploy a malicious payload, which is typically an Android Trojan. The MD5 hash of this BugDrop sample is 4b3c99ae792e7389c43102060633b4cc.
Strike BugDrop_ffd517d2	This strike sends a malware sample known as BugDrop. BugDrop is an Android malware that masquerades as a QR code scanner on the Google Play store. Its sole purpose is to bypass security measures used in the Google Play Store, and deploy a malicious payload, which is typically an Android Trojan. The MD5 hash of this BugDrop sample is ffd517d24a3d09082159493d859d4767.

<b>Name</b>	<b>Description</b>
Strike BugSleep_a50a20ed	This strike sends a malware sample known as BugSleep. BugSleep is a backdoor malware that has been associated with the Iranian threat group MuddyWater. It has the ability to execute commands, establish persistence, and transfer files between the target and the C2 server. The MD5 hash of this BugSleep sample is a50a20edddaded453410600549968914.
Strike BugSleep_a713e686	This strike sends a malware sample known as BugSleep. BugSleep is a backdoor malware that has been associated with the Iranian threat group MuddyWater. It has the ability to execute commands, establish persistence, and transfer files between the target and the C2 server. The MD5 hash of this BugSleep sample is a713e686fd984588a4db74f34bf32275.
Strike BugSleep_c17f4bb8	This strike sends a malware sample known as BugSleep. BugSleep is a backdoor malware that has been associated with the Iranian threat group MuddyWater. It has the ability to execute commands, establish persistence, and transfer files between the target and the C2 server. The MD5 hash of this BugSleep sample is c17f4bb8e415e21e6010b98e13c6dff3.
Strike BugSleep_d783001d	This strike sends a malware sample known as BugSleep. BugSleep is a backdoor malware that has been associated with the Iranian threat group MuddyWater. It has the ability to execute commands, establish persistence, and transfer files between the target and the C2 server. The MD5 hash of this BugSleep sample is d783001d1f98fe3b33e7b97b0b7d96dc.
Strike BugSleep_e7df84a5	This strike sends a malware sample known as BugSleep. BugSleep is a backdoor malware that has been associated with the Iranian threat group MuddyWater. It has the ability to execute commands, establish persistence, and transfer files between the target and the C2 server. The MD5 hash of this BugSleep sample is e7df84a5a22aeacf1c3abf4fd986c91.
Strike Bumblebee_171e9b04	This strike sends a polymorphic malware sample known as Bumblebee. Bumblebee is a downloader that contains anti-virtualization checks and the ability to download and execute other malicious payloads. Bumblebee has been associated with multiple campaigns, and has been known to deliver shellcode, Meterpreter, Silver and Cobalt Strike. The binary has the debug flag removed in the PE file format. The MD5 hash of this Bumblebee sample is 171e9b04a8b64c8b131c2d97bdc77879.
Strike Bumblebee_1fa7585f	This strike sends a malware sample known as Bumblebee. Bumblebee is a downloader that contains anti-virtualization checks and the ability to download and execute other malicious payloads. Bumblebee has been associated with multiple campaigns, and has been known to deliver shellcode, Meterpreter, Silver and Cobalt Strike. The MD5 hash of this Bumblebee sample is 1fa7585fa75b40c7aa52245d0cd13bc0.
Strike Bumblebee_21c886ea	This strike sends a polymorphic malware sample known as Bumblebee. Bumblebee is a downloader that contains anti-virtualization checks and the ability to download and execute other malicious payloads. Bumblebee has been associated with multiple campaigns, and has been known to deliver shellcode, Meterpreter, Silver and Cobalt Strike. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Bumblebee sample is 21c886eae8ce6dcef907160e430bba92.

<b>Name</b>	<b>Description</b>
Strike Bumblebee_23c611cb	This strike sends a polymorphic malware sample known as Bumblebee. Bumblebee is a downloader that contains anti-virtualization checks and the ability to download and execute other malicious payloads. Bumblebee has been associated with multiple campaigns, and has been known to deliver shellcode, Meterpreter, Silver and Cobalt Strike. The binary has random bytes appended at the end of the file. The MD5 hash of this Bumblebee sample is 23c611cb0d5f3d9d18f24eb1155d14da.
Strike Bumblebee_25a8caa9	This strike sends a polymorphic malware sample known as Bumblebee. Bumblebee is a downloader that contains anti-virtualization checks and the ability to download and execute other malicious payloads. Bumblebee has been associated with multiple campaigns, and has been known to deliver shellcode, Meterpreter, Silver and Cobalt Strike. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Bumblebee sample is 25a8caa929eb681e1f75b495e8ddbdde.
Strike Bumblebee_40a31230	This strike sends a malware sample known as Bumblebee. Bumblebee is a downloader that contains anti-virtualization checks and the ability to download and execute other malicious payloads. Bumblebee has been associated with multiple campaigns, and has been known to deliver shellcode, Meterpreter, Silver and Cobalt Strike. The MD5 hash of this Bumblebee sample is 40a312301d8462ef105bfc5ab26ba24d.
Strike Bumblebee_b3795bfd	This strike sends a malware sample known as Bumblebee. Bumblebee is a downloader that contains anti-virtualization checks and the ability to download and execute other malicious payloads. Bumblebee has been associated with multiple campaigns, and has been known to deliver shellcode, Meterpreter, Silver and Cobalt Strike. The MD5 hash of this Bumblebee sample is b3795bfd719bba20a0a258c8b49c4303.
Strike Bumblebee_d11663fa	This strike sends a polymorphic malware sample known as Bumblebee. Bumblebee is a downloader that contains anti-virtualization checks and the ability to download and execute other malicious payloads. Bumblebee has been associated with multiple campaigns, and has been known to deliver shellcode, Meterpreter, Silver and Cobalt Strike. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Bumblebee sample is d11663fa06c252e4601c21fc7233603c.
Strike Bumblebee_e6a046d1	This strike sends a malware sample known as Bumblebee. Bumblebee is a downloader that contains anti-virtualization checks and the ability to download and execute other malicious payloads. Bumblebee has been associated with multiple campaigns, and has been known to deliver shellcode, Meterpreter, Silver and Cobalt Strike. The MD5 hash of this Bumblebee sample is e6a046d1baa7cd2100bdf48102b8a144.
Strike Bumblebee_f225b34f	This strike sends a polymorphic malware sample known as Bumblebee. Bumblebee is a downloader that contains anti-virtualization checks and the ability to download and execute other malicious payloads. Bumblebee has been associated with multiple campaigns, and has been known to deliver shellcode, Meterpreter, Silver and Cobalt Strike. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Bumblebee sample is f225b34ffcf75bcd79a6dfc6a55c4d94.

<b>Name</b>	<b>Description</b>
Strike Bunitu_09126060	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 09126060aac595665a43eb4bdf868d8e.
Strike Bunitu_0b1fbf7b	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 0b1fbf7b3d1ec2a4ba50ee98e652f034.
Strike Bunitu_0c52ea60	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 0c52ea60269297afb478f67d2ab5d56d.
Strike Bunitu_0dd8a8bb	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 0dd8a8bbce09b241d3714e381a97698c.
Strike Bunitu_10abbb30	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 10abbb302916d3cb131ccf0f055a4c41.
Strike Bunitu_1f954e9f	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 1f954e9fabef22e942d65f42df913829d.
Strike Bunitu_2dcaf006	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 2dcaf006edc73c07bf6411ded128a819.
Strike Bunitu_2ef2abf8	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 2ef2abf85fd08fdf9088f6a771a43fa6.
Strike Bunitu_3dc09cda	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 3dc09cda71de69e01373c7c816b48af0.
Strike Bunitu_3f8f3288	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 3f8f3288cff60a0561800bb0e951ce6b.
Strike Bunitu_63211e86	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 63211e8682624e17ef3f669f99fa8163.
Strike Bunitu_6b70f387	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 6b70f387288e9314d9b99bb9332c8cfb.

<b>Name</b>	<b>Description</b>
Strike Bunitu_72541f06	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 72541f060e7ffea8b4157716d30865a8.
Strike Bunitu_841e52bb	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 841e52bb260a1ef424d4ecc95c143070.
Strike Bunitu_89763cd7	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is 89763cd7d46548e6eb2d0a4d1e1b3189.
Strike Bunitu_ad2714b9	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is ad2714b9dde080b8ef42a9cef4849d09.
Strike Bunitu_b0780dc0	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is b0780dc0ad57ec5dd2f39cf6f1e1f982.
Strike Bunitu_b678f0a6	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is b678f0a64be441e9a6019c8449964810.
Strike Bunitu_b8ddc49f	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is b8ddc49fe95c03a93525cfa639311c26.
Strike Bunitu_c44d6817	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is c44d6817a42bc4fbcaefd6ce1578382f.
Strike Bunitu_ce9f92d5	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is ce9f92d5455b07aa4210fe3c7de5fc4b.
Strike Bunitu_d3803b27	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is d3803b27b2a10ed70770708bcba62247.
Strike Bunitu_ff3441a1	This strike sends a malware sample known as Bunitu. Once Bunitu establishes persistence on the system it turns that machine into a proxy for malicious VPN services. The MD5 hash of this Bunitu sample is ff3441a1eb4584774b6e1b09f5bdf6fd.

<b>Name</b>	<b>Description</b>
Strike CLOP_508a671c	<p>This strike sends a polymorphic malware sample known as CLOP. CLOP ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The binary has the checksum removed in the PE file format. The MD5 hash of this CLOP sample is 508a671cf24f381582459ccda863d520.</p>
Strike CLOP_9ec70a82	<p>This strike sends a polymorphic malware sample known as CLOP. CLOP ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The binary has been packed using upx packer, with the default options. The MD5 hash of this CLOP sample is 9ec70a82f8b4797c4ad4fe646cfb6e10.</p>
Strike CLOP_a04eb443	<p>This strike sends a malware sample known as CLOP. CLOP ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The MD5 hash of this CLOP sample is a04eb443870896fbe9a0b6468c4844f7.</p>
Strike CLOP_d3ace85c	<p>This strike sends a polymorphic malware sample known as CLOP. CLOP ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this CLOP sample is d3ace85c17df113fa90a92a541ff0ca7.</p>
Strike CLOP_f2114603	<p>This strike sends a malware sample known as CLOP. CLOP ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The MD5 hash of this CLOP sample is f21146030cbe2ebe5a8e3fd67df8e8f3.</p>
Strike CaddyWiper_01fe1c58	<p>This strike sends a polymorphic malware sample known as CaddyWiper. CaddyWiper is a Ukraine targeted, relatively small in size wiper malware with the purpose of destroying all the contents of a system's drives. Before erasing these files it checks that the machine is not a domain controller, and if it is it will halt execution. If it is not a dc it will continue by wiping files on each drive on the system. The binary has random bytes appended at the end of the file. The MD5 hash of this CaddyWiper sample is 01fe1c580fdd0837b8119953689aa1ae.</p>

<b>Name</b>	<b>Description</b>
Strike CaddyWiper_1dc1b969	This strike sends a polymorphic malware sample known as CaddyWiper. CaddyWiper is a Ukraine targeted, relatively small in size wiper malware with the purpose of destroying all the contents of a system's drives. Before erasing these files it checks that the machine is not a domain controller, and if it is it will halt execution. If it is not a dc it will continue by wiping files on each drive on the system. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this CaddyWiper sample is 1dc1b96929eda836f0461b13b23ef173.
Strike CaddyWiper_3a4b1c1f	This strike sends a malware sample known as CaddyWiper. CaddyWiper is a Ukraine targeted, relatively small in size wiper malware with the purpose of destroying all the contents of a system's drives. Before erasing these files it checks that the machine is not a domain controller, and if it is it will halt execution. If it is not a dc it will continue by wiping files on each drive on the system. The MD5 hash of this CaddyWiper sample is 3a4b1c1f68811b38be74e99e572efae9.
Strike CaddyWiper_3bac736d	This strike sends a malware sample known as CaddyWiper. CaddyWiper is a Ukraine targeted, relatively small in size wiper malware with the purpose of destroying all the contents of a system's drives. Before erasing these files it checks that the machine is not a domain controller, and if it is it will halt execution. If it is not a dc it will continue by wiping files on each drive on the system. The MD5 hash of this CaddyWiper sample is 3bac736dfc996976ebd089338cf38c8b.
Strike CaddyWiper_3d2ef2ef	This strike sends a polymorphic malware sample known as CaddyWiper. CaddyWiper is a Ukraine targeted, relatively small in size wiper malware with the purpose of destroying all the contents of a system's drives. Before erasing these files it checks that the machine is not a domain controller, and if it is it will halt execution. If it is not a dc it will continue by wiping files on each drive on the system. The binary has been packed using upx packer, with the default options. The MD5 hash of this CaddyWiper sample is 3d2ef2ef006e37aa4e7aed84d33f243c.
Strike CaddyWiper_42e2b6e4	This strike sends a malware sample known as CaddyWiper. CaddyWiper is a Ukraine targeted, relatively small in size wiper malware with the purpose of destroying all the contents of a system's drives. Before erasing these files it checks that the machine is not a domain controller, and if it is it will halt execution. If it is not a dc it will continue by wiping files on each drive on the system. The MD5 hash of this CaddyWiper sample is 42e2b6e4fba51ec71235e28ddff27a76.
Strike CaddyWiper_42e52b8d	This strike sends a malware sample known as CaddyWiper. CaddyWiper is a Ukraine targeted, relatively small in size wiper malware with the purpose of destroying all the contents of a system's drives. Before erasing these files it checks that the machine is not a domain controller, and if it is it will halt execution. If it is not a dc it will continue by wiping files on each drive on the system. The MD5 hash of this CaddyWiper sample is 42e52b8daf63e6e26c3aa91e7e971492.

<b>Name</b>	<b>Description</b>
Strike CaddyWiper_b8da675f	This strike sends a polymorphic malware sample known as CaddyWiper. CaddyWiper is a Ukraine targeted, relatively small in size wiper malware with the purpose of destroying all the contents of a system's drives. Before erasing these files it checks that the machine is not a domain controller, and if it is it will halt execution. If it is not a dc it will continue by wiping files on each drive on the system. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this CaddyWiper sample is b8da675f41ea93ea27c76db661bc095d.
Strike CaddyWiper_da4ae5cf	This strike sends a polymorphic malware sample known as CaddyWiper. CaddyWiper is a Ukraine targeted, relatively small in size wiper malware with the purpose of destroying all the contents of a system's drives. Before erasing these files it checks that the machine is not a domain controller, and if it is it will halt execution. If it is not a dc it will continue by wiping files on each drive on the system. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this CaddyWiper sample is da4ae5cf38e4cef1113a7acc04830d2d.
Strike CastleRAT_14610b22	This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is 14610b22a749a0cd464d1985abbff45f.
Strike CastleRAT_22b5bf29	This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is 22b5bf2931140fae49228ced1d1dd3d7.
Strike CastleRAT_35f81d06	This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is 35f81d066028f5e69508956bed79d3ee.

<b>Name</b>	<b>Description</b>
Strike CastleRAT_669fce84	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is 669fce84d112e62291e96f49d42be557.</p>
Strike CastleRAT_9e21fbc9	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is 9e21fbc9e7862fb0d8ba59cf0f16037c.</p>
Strike CastleRAT_a0e6555a	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is a0e6555acf7d7a273b76067f89884705.</p>
Strike CastleRAT_ac77ab1a	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is ac77ab1a3f5a3691e23265bc495e84e8.</p>
Strike CastleRAT_bd61d42f	<p>This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is bd61d42f552a7288cfb474498f2f43fc.</p>

Name	Description
Strike CastleRAT_c7fed6e5	This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is c7fed6e5ad87ab5c13163300f2dfa500.
Strike CastleRAT_ce7e6656	This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is ce7e6656eb256a8b750097ff8e90ade5.
Strike CastleRAT_d195e390	This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is d195e39044641f3b1f74843318bca182.
Strike CastleRAT_f1ecdad8	This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is f1ecdad8fda4bdaa29fbda8f946a8e47.
Strike CastleRAT_f6ebab2c	This strike sends a malware sample known as CastleRAT. CastleRAT is a malware of the Remote Access Trojan (RAT) family that targets primarily Ukrainian entities. It is delivered through a loader, CastleLoader, which is distributed via malicious Microsoft Word documents. Upon execution, it establishes persistence on the victim's machine, collects system information, and communicates with a command-and-control server. Its key capabilities include executing arbitrary commands, uploading and downloading files, and keylogging, all controlled remotely by the attacker. The MD5 hash of this CastleRAT sample is f6ebab2c29256aaca8f8b8b6da89e6eb.
Strike Cerber_02a86e7e	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 02a86e7e82925efcbb3c63da2b73bbb6.

<b>Name</b>	<b>Description</b>
Strike Cerber_047b31ba	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 047b31ba3dfe6a21c2249f646b178cc7.
Strike Cerber_0a740a35	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has a new section added in the PE file format with random contents." The MD5 hash of this Cerber sample is 0a740a3523f8919bc4a3b18324b56b11.
Strike Cerber_10c96c50	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 10c96c50b1f8df439831cbc7f429313e.
Strike Cerber_14b76732	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has random strings (lorem ipsum) appended at the end of the file." The MD5 hash of this Cerber sample is 14b7673262e53efec58245abf183e38e.
Strike Cerber_17577ca7	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 17577ca743581e2ed7d4d26fc398f1ae.
Strike Cerber_1932244b	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has random contents appended in one of the existing sections in the PE file format." The MD5 hash of this Cerber sample is 1932244b79a2d4bc5b1bd062cc3d9aca.
Strike Cerber_1aad04ed	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 1aad04edca15d3323f8cdf31accf7a29.
Strike Cerber_1cb05585	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 1cb05585c3264a6c3c70d9c56c4792ce.
Strike Cerber_20fce6d	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 20fce6d01f396ae919275b8f48af3de.
Strike Cerber_253d7923	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 253d792321010b87432e04560dbdf645.
Strike Cerber_25ad9615	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has random bytes appended at the end of the file." The MD5 hash of this Cerber sample is 25ad961577215ecc0c998448528c5009.

<b>Name</b>	<b>Description</b>
Strike Cerber_26deaff2	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 26deaff26ac1591b8bd7786f5f481ab2.
Strike Cerber_271c2d2c	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber". The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Cerber sample is 271c2d2c8487d35a5d40f5b15a4f8382.
Strike Cerber_273bd74c	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber". The binary has been packed using upx packer, with the default options. The MD5 hash of this Cerber sample is 273bd74c8b4e5896e10233a4d3b97d8e.
Strike Cerber_2b3326a6	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 2b3326a68b949d19c8862de743303d03.
Strike Cerber_2ecc1dd8	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 2ecc1dd8dc81eed88244e714caa65f7.
Strike Cerber_2eee085c	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber". The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Cerber sample is 2eee085c6fb1e7d011252f3d1f94a0bf.
Strike Cerber_2f8da4f1	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber". The binary has been packed using upx packer, with the default options. The MD5 hash of this Cerber sample is 2f8da4f15e7407aaada1536cc08bc677.
Strike Cerber_357fa294	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 357fa29417f08554998886d0085d7739.
Strike Cerber_360dde65	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 360dde65f7547c1b9993e31e2c72fdab.
Strike Cerber_3a12510f	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 3a12510f6ef22cf3bbeeb91eda2e8bf8.

<b>Name</b>	<b>Description</b>
Strike Cerber_3a7d6f4b	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 3a7d6f4b69fbb77653d6b66f60289f8a.
Strike Cerber_41732f62	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 41732f6244f7d05554fe973021aefcc7.
Strike Cerber_42acf5ec	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 42acf5ecf3d8d4762899bcc11216e97e.
Strike Cerber_474b8477	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 474b84770337af1417e00febddd09b2.
Strike Cerber_4d71d738	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 4d71d738887d2bc046f732bf1f13391c.
Strike Cerber_50639679	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 50639679fad036720738b11c52792c9e.
Strike Cerber_51bd27fb	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 51bd27fb47b75f383d45a28ed723c87e.
Strike Cerber_53d0d6a8	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 53d0d6a85e1c7722ab507955473438dd.
Strike Cerber_566d6f54	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 566d6f54aefed24a394a62e2e6990cc5.
Strike Cerber_5795839f	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 5795839fe075e11bcf84a6e0468a3190.
Strike Cerber_59bfd7c1	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 59bfd7c1e780c9fb0cb65860e492857a.
Strike Cerber_5a04902f	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has been packed using upx packer, with the default options." The MD5 hash of this Cerber sample is 5a04902f4a5f4993df449721e689eb00.

<b>Name</b>	<b>Description</b>
Strike Cerber_5a381543	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 5a3815434730fab61a38265930c678f9.
Strike Cerber_5f26d3ae	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has random contents appended in one of the existing sections in the PE file format." The MD5 hash of this Cerber sample is 5f26d3ae3848b9be74dcec5fbff55b98.
Strike Cerber_6167a99c	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 6167a99ceadd1db397f645de514e0430.
Strike Cerber_652646a3	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has random bytes appended at the end of the file." The MD5 hash of this Cerber sample is 652646a346118252e84985f3435d8ad3.
Strike Cerber_65fb1282	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 65fb1282da1e3118c18b737f200ffab2.
Strike Cerber_66199b13	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 66199b1353550d116ac61e47c91986a7.
Strike Cerber_672aacd3	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has the timestamp field updated in the PE file header." The MD5 hash of this Cerber sample is 672aacd37d986db6c91eeb3702bef3ba.
Strike Cerber_69978e23	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 69978e2336e5bf01fc795f319eb36b0a.
Strike Cerber_6b9989b7	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 6b9989b765f5bd4fa78700f05b81fff6.
Strike Cerber_6f518175	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 6f5181752a3e47b0671cd8579143fe36.
Strike Cerber_70a3a2a8	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 70a3a2a8d3c916b2ec01d5d7dcd6c3bf.

<b>Name</b>	<b>Description</b>
Strike Cerber_70a6b557	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 70a6b557d71dce9f22bef86f5344629b.
Strike Cerber_71785297	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber". The binary has the timestamp field updated in the PE file header. The MD5 hash of this Cerber sample is 71785297665f915f985e52f395678c35.
Strike Cerber_73c8594c	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 73c8594c223cf57288e84515b47f697d.
Strike Cerber_78df79ec	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 78df79ec2d06ab8cdb08f6ff59f23007.
Strike Cerber_7c4d7506	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 7c4d7506133b8cd8d584c703ff5364d2.
Strike Cerber_8ab540d5	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber.The binary has random bytes appended at the end of the file." The MD5 hash of this Cerber sample is 8ab540d55a63245b71a82a1a2ffa0016.
Strike Cerber_8baa9694	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 8baa96945edfd47b00622762f66af5ff.
Strike Cerber_8dfe6b10	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 8dfe6b105318375008b739f597ddd0bd.
Strike Cerber_8e3ff00e	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 8e3ff00e2f4ffb177b991b68f8975001.
Strike Cerber_8ee43cab	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 8ee43cab50aaeb5797a8785c334b4873.
Strike Cerber_918ee14f	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 918ee14fe18157490c2c32d79bc9fe80.

<b>Name</b>	<b>Description</b>
Strike Cerber_93b1e1dc	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 93b1e1dcbfe3389af820e092e0890067.
Strike Cerber_94a8e68b	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 94a8e68bea0dd0bee6310d7326aff82c.
Strike Cerber_94b1351c	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 94b1351c99fa4c5229fd1b5bae7578ba.
Strike Cerber_94c9da20	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 94c9da203a24f64aa998239e3d25d70c.
Strike Cerber_98e34f3c	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 98e34f3c420bc904f471f9ffed00d61c.
Strike Cerber_99046243	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary file has one more imports added in the import table." The MD5 hash of this Cerber sample is 99046243810bff30981aa756db7a9432.
Strike Cerber_9cc74544	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has a random section name renamed according to the PE format specification." The MD5 hash of this Cerber sample is 9cc74544cc2abb9647f3894215f65124.
Strike Cerber_9d225aba	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 9d225abad306db39bb37c6c4e9ccbe17.
Strike Cerber_9d8910be	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 9d8910bec8f05fefebf96fca21c685e4.
Strike Cerber_9f2a535d	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is 9f2a535d3d35f990f291c3bbb0c0fc8a.
Strike Cerber_a084f960	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a084f96088ac607afafa8a41fae13449.

<b>Name</b>	<b>Description</b>
Strike Cerber_a0a620a9	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a0a620a900c4a3fc42db9c2632f55a96.
Strike Cerber_a0e22f8b	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a0e22f8b2be97dd7f539209350aabaf5.
Strike Cerber_a1456115	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a1456115c9688f5792bdcd2723764f9c.
Strike Cerber_a1652735	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a16527350f21508630e955fc6efab7d8.
Strike Cerber_a2656455	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a26564559325bccd013c7db518e2f4d6.
Strike Cerber_a2c19fe2	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a2c19fe2ebdc074bf4c533cc929f2da9.
Strike Cerber_a316e709	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a316e70955be20426f5d2a12f5bfeaa8.
Strike Cerber_a40ee742	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a40ee74258c0f9d49dc18bc4dd27df93.
Strike Cerber_a42c9151	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a42c91514cbd1eb343e69c1ce2aa0f81.
Strike Cerber_a477662e	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a477662edef8ab16496caf23a208250f.
Strike Cerber_a5741d01	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a5741d01be4d0cc52fc4988a6337a834.
Strike Cerber_a6fe0fda	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a6fe0fda24d5a34b151ba42d11d3af2b.

<b>Name</b>	<b>Description</b>
Strike Cerber_a7b5ca0a	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a7b5ca0afd68452ccfa9f037936f06f5.
Strike Cerber_a80f27b1	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a80f27b1d8de0ba006b57db694225cd0.
Strike Cerber_a8aa7411	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a8aa7411837c2341c9c281d60c18a934.
Strike Cerber_a916a0a7	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a916a0a7a6efbc763d8f3e7efbcfb631.
Strike Cerber_a98f80cc	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is a98f80cc868e0913f9c7c42d4162447e.
Strike Cerber_aa038ee8	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is aa038ee865d3da0373c92a693bcc1459.
Strike Cerber_aae16290	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is aae16290207f1251b6b9510a50760323.
Strike Cerber_ae6e64f2	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is ae6e64f2fe99eea396b7167192c091f8.
Strike Cerber_ae7d7901	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is ae7d7901de45faca15a9575b702cea61.
Strike Cerber_aed47450	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is aed474509baeb1b716d5c65d21a2cfc.
Strike Cerber_af19eac8	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is af19eac84be5efd362b46e15930cc538.
Strike Cerber_af26a65a	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is af26a65adeef251c7ee04c4457d2135d.

<b>Name</b>	<b>Description</b>
Strike Cerber_af77aefb	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is af77aefb38535197e5551c0549beeb7c.
Strike Cerber_b055cf6b	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is b055cf6b4059ac70de7497ee0ae501c5.
Strike Cerber_b3923fb7	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is b3923fb72ad8b7ca15ad85d7082a1429.
Strike Cerber_b50ff227	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has random contents appended in one of the existing sections in the PE file format." The MD5 hash of this Cerber sample is b50ff227c1bf3f5091c90abf54dfade1.
Strike Cerber_b54b348b	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is b54b348b1d7081f03c73e4b6ddc647bd.
Strike Cerber_b7549aee	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is b7549aee594d32bcc4a8389b77ae412b.
Strike Cerber_b99039f7	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is b99039f7536a9500dd0f0e45f4619e27.
Strike Cerber_b9a116e6	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is b9a116e602ac51e388b56b5769065af6.
Strike Cerber_b9a78094	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is b9a78094607d6b3e2b6b46076a954cb5.
Strike Cerber_ba2cb51a	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is ba2cb51a7d5946eaee662404c55fc180.
Strike Cerber_be17b86e	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is be17b86ef5b9f814b3039ddffabaaed5.
Strike Cerber_bebf0baef	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is bebf0bafbaec81602551b9ebe345a15f.

<b>Name</b>	<b>Description</b>
Strike Cerber_bf37d4ed	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is bf37d4ed20b512c1e8c1073c4c91e330.
Strike Cerber_c01e7329	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is c01e73294c167d28d9b2a7bd234aa03f.
Strike Cerber_c02251f7	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has a random section name renamed according to the PE format specification." The MD5 hash of this Cerber sample is c02251f76df02d8e41f2601342a30e8a.
Strike Cerber_c40b891e	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is c40b891ea6021a7a704a75fcf049e0d2.
Strike Cerber_c48a35cf	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is c48a35cf1626e9cd2f2a4e5b2493790e.
Strike Cerber_c80008df	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is c80008df5fa7cb0f90f41a151b35e653.
Strike Cerber_ca873bae	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is ca873baed524d16a6c1050b0a5a2df22.
Strike Cerber_cb6cc5ad	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is cb6cc5ad90de92dbe93b85ee09be620f.
Strike Cerber_cb6d7b58	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is cb6d7b58eec5efe3fa44c873529e7db0.
Strike Cerber_ce478d86	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is ce478d8638a31fd6593c31ceb29fdad2.
Strike Cerber_cf0444a7	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is cf0444a7ea6bede0449c90bbcb92d113.
Strike Cerber_d08b6626	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is d08b6626b95874a16a0b4aee087b9536.

<b>Name</b>	<b>Description</b>
Strike Cerber_d1d5145d	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is d1d5145da3dde367f9a84b3f23c0e399.
Strike Cerber_d5b9760f	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is d5b9760f25cc8466995b30e005438e14.
Strike Cerber_d6532b4f	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is d6532b4f98349e6ccb013c250be1a857.
Strike Cerber_d8AAF63d	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is d8AAF63dd0d7e7a646e8edc7fcc09f87.
Strike Cerber_d91c1f6a	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is d91c1f6a864b069544a731a22c22ec8f.
Strike Cerber_da7caa79	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has been packed using upx packer, with the default options. The MD5 hash of this Cerber sample is da7caa79b0c87a2f3360d959cc1e1637.
Strike Cerber_dbe1d59a	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is dbe1d59af02ee4e9ad739f6261b01648.
Strike Cerber_dc82432a	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is dc82432a6a69957fcc2e326fb97924a.
Strike Cerber_de16708e	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is de16708e8edb9e4300b83905a5de7760.
Strike Cerber_de77b672	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is de77b6722ec5f99fc2e5d562ebb6e864.
Strike Cerber_e0510f6d	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is e0510f6d847bffd75988a25a5bb77b14.

<b>Name</b>	<b>Description</b>
Strike Cerber_e122bb15	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is e122bb15a9fe5912c2812e5517760477.
Strike Cerber_e3246475	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is e3246475a537b99f2ae00903e3d3513a.
Strike Cerber_e45eff55	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary file has one more imports added in the import table." The MD5 hash of this Cerber sample is e45eff551e16ff88fc4e224046dc82ee.
Strike Cerber_e49cf5e5	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is e49cf5e5319316e985c17691d7a6c71d.
Strike Cerber_eb93bc01	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is eb93bc01bdef478ac35d87f0d7caf01c.
Strike Cerber_ebf48e14	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is ebf48e14acaa333bc1049b9fd09838f0.
Strike Cerber_edc7fd66	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has the checksum removed in the PE file format." The MD5 hash of this Cerber sample is edc7fd66d1ffb2f1504a1eac4495e875.
Strike Cerber_f0508ea4	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is f0508ea416765b1c9f7af84bfbb2b2d1.
Strike Cerber_f4d3549a	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is f4d3549ad343726b7dc618be7122732d.
Strike Cerber_f633f7b4	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is f633f7b424983cef70eae8bcbf81ff19.
Strike Cerber_f6486529	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is f6486529e6ae82d03dca5889ff20e8d7.
Strike Cerber_f64c231c	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is f64c231cc0d3334289192c8e571c70a2.

<b>Name</b>	<b>Description</b>
Strike Cerber_f6d34c87	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is f6d34c87bc644ef81d8cf6bcfa53f851.
Strike Cerber_f902f4a5	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is f902f4a5f05146167eфеаed2a8f7961c.
Strike Cerber_f99d1b2f	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has random strings (lorem ipsum) appended at the end of the file." The MD5 hash of this Cerber sample is f99d1b2fae036d1dc72c13c075961d14.
Strike Cerber_fb4af472	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber". The binary has random bytes appended at the end of the file. The MD5 hash of this Cerber sample is fb4af472afa96bd412d67b9080699494.
Strike Cerber_fbd66faf	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is fbd66faff99a1b8f056a6075b512621e.
Strike Cerber_fce00a14	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is fce00a14d4542ddada0bebfoa40cb7ea.
Strike Cerber_fe03f656	This strike sends a malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The MD5 hash of this Cerber sample is fe03f656cc2a508f3bedaa131fe9509c.
Strike Cerber_fe2ccd90	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has random contents appended in one of the existing sections in the PE file format." The MD5 hash of this Cerber sample is fe2ccd90af759a48ec678af945fb84c5.
Strike Cerber_fffb908e	This strike sends a polymorphic malware sample known as Cerber. Cerber is ransomware that encrypts documents, photos, databases and other important files using the file extension ".cerber." The binary has random strings (lorem ipsum) appended at the end of the file." The MD5 hash of this Cerber sample is fffb908eff59f3dc30b3f6a785102bcc.

<b>Name</b>	<b>Description</b>
Strike ChaosRAT_30598ea4	<p>This strike sends a malware sample known as Chaos RAT. This strike sends a malware sample known as Chaos RAT. Chaos RAT is a cross-platform remote access trojan written in Golang that targets both Windows and Linux systems. It is delivered through phishing campaigns and disguises itself as legitimate tools such as network analyzers. Once executed, the malware establishes communication with a command and control server using encoded configuration files and JWT tokens. It allows attackers to run system commands, capture screenshots, exfiltrate files, and deploy cryptocurrency miners. Chaos RAT also uses obfuscation techniques and sets up persistence through scheduled tasks on Windows or cron jobs on Linux. The MD5 hash of this Chaos RAT sample is 30598ea49a58838e3bea367e89653202.</p>
Strike ChaosRAT_653c7a95	<p>This strike sends a malware sample known as Chaos RAT. This strike sends a malware sample known as Chaos RAT. Chaos RAT is a cross-platform remote access trojan written in Golang that targets both Windows and Linux systems. It is delivered through phishing campaigns and disguises itself as legitimate tools such as network analyzers. Once executed, the malware establishes communication with a command and control server using encoded configuration files and JWT tokens. It allows attackers to run system commands, capture screenshots, exfiltrate files, and deploy cryptocurrency miners. Chaos RAT also uses obfuscation techniques and sets up persistence through scheduled tasks on Windows or cron jobs on Linux. The MD5 hash of this Chaos RAT sample is 653c7a95e4d03518f8995cf05a0b4c36.</p>
Strike ChaosRAT_69656a3d	<p>This strike sends a malware sample known as Chaos RAT. This strike sends a malware sample known as Chaos RAT. Chaos RAT is a cross-platform remote access trojan written in Golang that targets both Windows and Linux systems. It is delivered through phishing campaigns and disguises itself as legitimate tools such as network analyzers. Once executed, the malware establishes communication with a command and control server using encoded configuration files and JWT tokens. It allows attackers to run system commands, capture screenshots, exfiltrate files, and deploy cryptocurrency miners. Chaos RAT also uses obfuscation techniques and sets up persistence through scheduled tasks on Windows or cron jobs on Linux. The MD5 hash of this Chaos RAT sample is 69656a3d7555db170554fc7689fffc2b.</p>
Strike ChaosRAT_88c465d1	<p>This strike sends a malware sample known as Chaos RAT. This strike sends a malware sample known as Chaos RAT. Chaos RAT is a cross-platform remote access trojan written in Golang that targets both Windows and Linux systems. It is delivered through phishing campaigns and disguises itself as legitimate tools such as network analyzers. Once executed, the malware establishes communication with a command and control server using encoded configuration files and JWT tokens. It allows attackers to run system commands, capture screenshots, exfiltrate files, and deploy cryptocurrency miners. Chaos RAT also uses obfuscation techniques and sets up persistence through scheduled tasks on Windows or cron jobs on Linux. The MD5 hash of this Chaos RAT sample is 88c465d1a85d4b4beeedb52c7f7dfaed.</p>

<b>Name</b>	<b>Description</b>
Strike ChaosRAT_aaa95a74	<p>This strike sends a malware sample known as Chaos RAT. This strike sends a malware sample known as Chaos RAT. Chaos RAT is a cross-platform remote access trojan written in Golang that targets both Windows and Linux systems. It is delivered through phishing campaigns and disguises itself as legitimate tools such as network analyzers. Once executed, the malware establishes communication with a command and control server using encoded configuration files and JWT tokens. It allows attackers to run system commands, capture screenshots, exfiltrate files, and deploy cryptocurrency miners. Chaos RAT also uses obfuscation techniques and sets up persistence through scheduled tasks on Windows or cron jobs on Linux. The MD5 hash of this Chaos RAT sample is aaa95a7470abc3b25b541aa6e0c4b7c1.</p>
Strike ChaosRAT_c8f89850	<p>This strike sends a malware sample known as Chaos RAT. This strike sends a malware sample known as Chaos RAT. Chaos RAT is a cross-platform remote access trojan written in Golang that targets both Windows and Linux systems. It is delivered through phishing campaigns and disguises itself as legitimate tools such as network analyzers. Once executed, the malware establishes communication with a command and control server using encoded configuration files and JWT tokens. It allows attackers to run system commands, capture screenshots, exfiltrate files, and deploy cryptocurrency miners. Chaos RAT also uses obfuscation techniques and sets up persistence through scheduled tasks on Windows or cron jobs on Linux. The MD5 hash of this Chaos RAT sample is c8f89850cfeeada08b46a23c45c7957d.</p>
Strike ChaosRAT_e502b8d6	<p>This strike sends a malware sample known as Chaos RAT. This strike sends a malware sample known as Chaos RAT. Chaos RAT is a cross-platform remote access trojan written in Golang that targets both Windows and Linux systems. It is delivered through phishing campaigns and disguises itself as legitimate tools such as network analyzers. Once executed, the malware establishes communication with a command and control server using encoded configuration files and JWT tokens. It allows attackers to run system commands, capture screenshots, exfiltrate files, and deploy cryptocurrency miners. Chaos RAT also uses obfuscation techniques and sets up persistence through scheduled tasks on Windows or cron jobs on Linux. The MD5 hash of this Chaos RAT sample is e502b8d617a2cd9bfa41762282a0ff81.</p>
Strike ChaosRAT_ee890d42	<p>This strike sends a malware sample known as Chaos RAT. This strike sends a malware sample known as Chaos RAT. Chaos RAT is a cross-platform remote access trojan written in Golang that targets both Windows and Linux systems. It is delivered through phishing campaigns and disguises itself as legitimate tools such as network analyzers. Once executed, the malware establishes communication with a command and control server using encoded configuration files and JWT tokens. It allows attackers to run system commands, capture screenshots, exfiltrate files, and deploy cryptocurrency miners. Chaos RAT also uses obfuscation techniques and sets up persistence through scheduled tasks on Windows or cron jobs on Linux. The MD5 hash of this Chaos RAT sample is ee890d42d22257205001cd9586bfa7d2.</p>

<b>Name</b>	<b>Description</b>
Strike ChaosRAT_f9ed313b	This strike sends a malware sample known as Chaos RAT. This strike sends a malware sample known as Chaos RAT. Chaos RAT is a cross-platform remote access trojan written in Golang that targets both Windows and Linux systems. It is delivered through phishing campaigns and disguises itself as legitimate tools such as network analyzers. Once executed, the malware establishes communication with a command and control server using encoded configuration files and JWT tokens. It allows attackers to run system commands, capture screenshots, exfiltrate files, and deploy cryptocurrency miners. Chaos RAT also uses obfuscation techniques and sets up persistence through scheduled tasks on Windows or cron jobs on Linux. The MD5 hash of this Chaos RAT sample is f9ed313b6414a9a761743dc90defc59f.
Strike ChaosRAT_fab45026	This strike sends a malware sample known as Chaos RAT. This strike sends a malware sample known as Chaos RAT. Chaos RAT is a cross-platform remote access trojan written in Golang that targets both Windows and Linux systems. It is delivered through phishing campaigns and disguises itself as legitimate tools such as network analyzers. Once executed, the malware establishes communication with a command and control server using encoded configuration files and JWT tokens. It allows attackers to run system commands, capture screenshots, exfiltrate files, and deploy cryptocurrency miners. Chaos RAT also uses obfuscation techniques and sets up persistence through scheduled tasks on Windows or cron jobs on Linux. The MD5 hash of this Chaos RAT sample is fab450261c2e3d86f6b8b005d76a9b85.
Strike ChatGPT-SmsMalware_8468af0e	This strike sends an Android malware sample which sample poses as a ChatGPT app. It's a SMS malware which performs billing fraud by sending SMS messages to premium numbers in an attempt to empty wallet of victims. 'com.chatgpt.ogothai' is the package name of the malware sample. The MD5 hash of this sample is 4e8d09ca0543a48f649fce72483777f0.
Strike ChatGPT-SmsMalware_da4df33c	This strike sends an Android polymorphic malware sample which sample poses as a ChatGPT app. It's a SMS malware which performs billing fraud by sending SMS messages to premium numbers in an attempt to empty wallet of victims. 'com.chatgpt.ogothai' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this sample is da4df33c3c6ea0e313d913a9a6df5856.
Strike ChatGPT-SmsMalware_ededa287	This strike sends an Android polymorphic malware sample which sample poses as a ChatGPT app. It's a SMS malware which performs billing fraud by sending SMS messages to premium numbers in an attempt to empty wallet of victims. 'com.chatgpt.ogothai' is the package name of the malware sample. The malware has been randomly rebuilt without any modifications. The MD5 hash of this sample is ededa2877f700a2dc8e1119ac59c85ea.
Strike Chthonic_07db0094	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is 07db009460cbefb77763f3dcf7559b89.

<b>Name</b>	<b>Description</b>
Strike Chthonic_35e71926	This strike sends a polymorphic malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Chthonic sample is 35e7192617a5bfe4e3663f40610a7f11.
Strike Chthonic_39a1430c	This strike sends a polymorphic malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Chthonic sample is 39a1430c7d0bf12a9b42dad4e6b49ac6.
Strike Chthonic_39e3d389	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is 39e3d389fa34b594117f49b38d602584.
Strike Chthonic_4ad3b625	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is 4ad3b625ebadf92523edc1b0730dba9a.
Strike Chthonic_562f8c4a	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is 562f8c4a3657b2afbd72f667965cf816.
Strike Chthonic_5e4a3caa	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is 5e4a3caaa954f755e77cb2e704abc62c.
Strike Chthonic_6f3520ec	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is 6f3520ece3ccfb8011b9545fd8dfd0c.

<b>Name</b>	<b>Description</b>
Strike Chthonic_7e665259	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is 7e665259f4178cfc254d809d3acfc2b2.
Strike Chthonic_a5cdcf1b	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is a5cdcf1b8a826d3fba2b892ae203d366.
Strike Chthonic_adb1e861	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is adb1e8619419ccaf530aa03e709d670a.
Strike Chthonic_af6c53ea	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is af6c53ea36ebdd113728e86798e930af.
Strike Chthonic_b4f83819	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is b4f8381988ce8b623949a5a64e547560.
Strike Chthonic_c020bae7	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is c020bae796d8a22ea7e7bf7985b3bb5f.
Strike Chthonic_d3bd502b	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is d3bd502b5eb378de043d15938f730b75.
Strike Chthonic_df156d22	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose to to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is df156d229e2f94fa017882015dae6129.

<b>Name</b>	<b>Description</b>
Strike Chthonic_eda8ab97	This strike sends a malware sample known as Chthonic. Chthonic is a banking trojan that is normally delivered by the attacker via phishing emails. Its purpose is to exfiltrate sensitive credentials from the victim machine, and has also been seen delivering other malware like AZORult to perform additional functionality. The MD5 hash of this Chthonic sample is eda8ab9741ff7b166c04d59e4c778a45.
Strike ClayRAT_0658b719	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 0658b719a2dcb7762743af4ea97646af.
Strike ClayRAT_074b5622	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 074b5622421e8ed778af7d0c013c365c.
Strike ClayRAT_0abb2947	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 0abb29472275a0d558839e3fb16a2407.
Strike ClayRAT_198505a6	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 198505a6ac0ff95b4f9cada0a7f7a393.
Strike ClayRAT_49e0f3d2	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 49e0f3d2284ed076ad5a72af97548fba.

<b>Name</b>	<b>Description</b>
Strike ClayRAT_57149137	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 57149137ee7145ad106cdac344e70c85.
Strike ClayRAT_5a0f7c94	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 5a0f7c94841306c309da7dc3045071e5.
Strike ClayRAT_698fd171	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 698fd1710d7fae4308022bf181d62b4d.
Strike ClayRAT_7c87ffd8	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 7c87ffd8dfd36ceedcf0e2a45f059c0b.
Strike ClayRAT_91a10457	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 91a10457b782945178c5c6a2f4c60123.
Strike ClayRAT_9bd27080	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is 9bd2708072b016777c412d475b8b6720.

<b>Name</b>	<b>Description</b>
Strike ClayRAT_aa5c7f83	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is aa5c7f832eb47c8b6acaf9fcbe87a699.
Strike ClayRAT_c5b7070e	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is c5b7070ee6e114e2311d200afdb0c804.
Strike ClayRAT_c8200034	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is c82000348c9b5a302bd5073b52c13221.
Strike ClayRAT_e2f3d7bc	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is e2f3d7bcd79bc500a64478977cb50efb.
Strike ClayRAT_e78cdced	This strike sends a malware sample known as ClayRAT. ClayRAT is a malware of the spyware family that turns infected mobile devices into distribution hubs for further malware attacks. It is primarily delivered via malicious SMS messages and Telegram links. Once executed, ClayRAT sends out numerous fraudulent messages containing malware-laden links to the victim's contact list. Its key capabilities include contact list access, message sending, and the ability to install and propagate additional malware. The MD5 hash of this ClayRAT sample is e78cdced64bc65e392faeed019812a62.
Strike Clop_06198fed	This strike sends a malware sample known as Clop. Clop ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The MD5 hash of this Clop sample is 06198fed029adbc90796ca6d83a67789.

<b>Name</b>	<b>Description</b>
Strike Clop_3c8041db	This strike sends a polymorphic malware sample known as Clop. Clop ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The binary file has one more imports added in the import table. The MD5 hash of this Clop sample is 3c8041db612aaae02f6a7817722d3860.
Strike Clop_5700ff4d	This strike sends a polymorphic malware sample known as Clop. Clop ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The binary has random bytes appended at the end of the file. The MD5 hash of this Clop sample is 5700ff4de05433adf34b7d953921309c.
Strike Clop_77e19f05	This strike sends a polymorphic malware sample known as Clop. Clop ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The binary has the debug flag removed in the PE file format. The MD5 hash of this Clop sample is 77e19f056443b6dbbcccc1336251a7e4.
Strike Clop_9609f431	This strike sends a malware sample known as Clop. Clop ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The MD5 hash of this Clop sample is 9609f431724b58e4830caa8edbe80762.
Strike Clop_a8cc764e	This strike sends a malware sample known as Clop. Clop ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The MD5 hash of this Clop sample is a8cc764e7c7a62a0fc26bbe3df31daa6.
Strike Clop_abdf4986	This strike sends a malware sample known as Clop. Clop ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The MD5 hash of this Clop sample is abdf498691f2b028bae0fa4276edc04b.

<b>Name</b>	<b>Description</b>
Strike Clop_cff8284f	This strike sends a polymorphic malware sample known as Clop. Clop ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The binary has been packed using upx packer, with the default options. The MD5 hash of this Clop sample is cff8284fc354db8d10f0b98c207a990a.
Strike Clop_df84820d	This strike sends a polymorphic malware sample known as Clop. Clop ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Clop sample is df84820d39d82e9b44b189046271e03d.
Strike Clop_eb846aab	This strike sends a polymorphic malware sample known as Clop. Clop ransomware was originally detected as a variant of the CryptoMix ransomware family. It currently targets entire networks instead of individual machines and even attempts to disable Windows Defender and other security tools. Before it begins encryption of the system, it disables target processes, which can include debuggers, text editors, IDEs, as well as a host of Windows processes like Windows 10 and Microsoft applications. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Clop sample is eb846aab3d964db15250f61d12d20dc0.
Strike CloudScout_166b0d75	This strike sends a malware sample known as CloudScout. CloudScout is a toolset that has been used by the Chinese aligned APT group Evasive Panda. This group's objective is cyber espionage against countries and organizations that would not be aligned with Chinese interests. CloudScout is a .NET framework that consists of several modules that target different services like Google Drive, Gmail, and Outlook. The malware attempts to steal data from these services through session cookies by hijacking authenticated sessions from web browsers. The MD5 hash of this CloudScout sample is 166b0d75858ec81744921b133d72ab2d.
Strike CloudScout_624d58a9	This strike sends a malware sample known as CloudScout. CloudScout is a toolset that has been used by the Chinese aligned APT group Evasive Panda. This group's objective is cyber espionage against countries and organizations that would not be aligned with Chinese interests. CloudScout is a .NET framework that consists of several modules that target different services like Google Drive, Gmail, and Outlook. The malware attempts to steal data from these services through session cookies by hijacking authenticated sessions from web browsers. The MD5 hash of this CloudScout sample is 624d58a9a56c0f0a5c4923557a99f808.

<b>Name</b>	<b>Description</b>
Strike CloudScout_6b32494a	This strike sends a malware sample known as CloudScout. CloudScout is a toolset that has been used by the Chinese aligned APT group Evasive Panda. This group's objective is cyber espionage against countries and organizations that would not be aligned with Chinese interests. CloudScout is a .NET framework that consists of several modules that target different services like Google Drive, Gmail, and Outlook. The malware attempts to steal data from these services through session cookies by hijacking authenticated sessions from web browsers. The MD5 hash of this CloudScout sample is 6b32494ab850f7b8e61d30085ab7dbd7.
Strike CloudScout_963f9805	This strike sends a malware sample known as CloudScout. CloudScout is a toolset that has been used by the Chinese aligned APT group Evasive Panda. This group's objective is cyber espionage against countries and organizations that would not be aligned with Chinese interests. CloudScout is a .NET framework that consists of several modules that target different services like Google Drive, Gmail, and Outlook. The malware attempts to steal data from these services through session cookies by hijacking authenticated sessions from web browsers. The MD5 hash of this CloudScout sample is 963f9805fa2867df5d3d328c863f9dfa.
Strike CloudScout_be17d056	This strike sends a malware sample known as CloudScout. CloudScout is a toolset that has been used by the Chinese aligned APT group Evasive Panda. This group's objective is cyber espionage against countries and organizations that would not be aligned with Chinese interests. CloudScout is a .NET framework that consists of several modules that target different services like Google Drive, Gmail, and Outlook. The malware attempts to steal data from these services through session cookies by hijacking authenticated sessions from web browsers. The MD5 hash of this CloudScout sample is be17d056039267973e36043c678a5d56.
Strike CloudScout_c02b6a7c	This strike sends a malware sample known as CloudScout. CloudScout is a toolset that has been used by the Chinese aligned APT group Evasive Panda. This group's objective is cyber espionage against countries and organizations that would not be aligned with Chinese interests. CloudScout is a .NET framework that consists of several modules that target different services like Google Drive, Gmail, and Outlook. The malware attempts to steal data from these services through session cookies by hijacking authenticated sessions from web browsers. The MD5 hash of this CloudScout sample is c02b6a7cc4f4da2d6956049b90ff53ba.
Strike CloudScout_c643ef13	This strike sends a malware sample known as CloudScout. CloudScout is a toolset that has been used by the Chinese aligned APT group Evasive Panda. This group's objective is cyber espionage against countries and organizations that would not be aligned with Chinese interests. CloudScout is a .NET framework that consists of several modules that target different services like Google Drive, Gmail, and Outlook. The malware attempts to steal data from these services through session cookies by hijacking authenticated sessions from web browsers. The MD5 hash of this CloudScout sample is c643ef13ab7d1f78c8a1fba2143311c0.

<b>Name</b>	<b>Description</b>
Strike CobaltStrike_0db5767d	<p>This strike sends a malware sample known as Cobalt Strike. This strike sends a malware sample known as a Cobalt Strike PowerShell loader. This malware is a PowerShell-based loader that decrypts and executes shellcode directly in memory to deliver a Cobalt Strike Beacon. It is distributed through a publicly accessible .ps1 script hosted on infrastructure associated with Chinese and Russian regions. The loader employs evasion techniques such as API hashing, dynamic function resolution, and forged User-Agent headers. It retrieves its second-stage payload from a Baidu Cloud Function endpoint and communicates with a Russian-hosted command and control server using a Cobalt Strike SSL certificate. The MD5 hash of this Cobalt Strike sample is 0db5767dba54e0e68ff26c585ce2e590.</p>
Strike CobaltStrike_58d5fc70	<p>This strike sends a malware sample known as Cobalt Strike. This strike sends a malware sample known as a Cobalt Strike PowerShell loader. This malware is a PowerShell-based loader that decrypts and executes shellcode directly in memory to deliver a Cobalt Strike Beacon. It is distributed through a publicly accessible .ps1 script hosted on infrastructure associated with Chinese and Russian regions. The loader employs evasion techniques such as API hashing, dynamic function resolution, and forged User-Agent headers. It retrieves its second-stage payload from a Baidu Cloud Function endpoint and communicates with a Russian-hosted command and control server using a Cobalt Strike SSL certificate. The MD5 hash of this Cobalt Strike sample is 58d5fc70e8aba11541272ad42ceb0e3a.</p>
Strike CobaltStrike_63b7b31a	<p>This strike sends a malware sample known as Cobalt Strike. This strike sends a malware sample known as a Cobalt Strike PowerShell loader. This malware is a PowerShell-based loader that decrypts and executes shellcode directly in memory to deliver a Cobalt Strike Beacon. It is distributed through a publicly accessible .ps1 script hosted on infrastructure associated with Chinese and Russian regions. The loader employs evasion techniques such as API hashing, dynamic function resolution, and forged User-Agent headers. It retrieves its second-stage payload from a Baidu Cloud Function endpoint and communicates with a Russian-hosted command and control server using a Cobalt Strike SSL certificate. The MD5 hash of this Cobalt Strike sample is 63b7b31a9436e8f965334ed07cbf2a34.</p>
Strike CobaltStrike_7e9fe1a8	<p>This strike sends a malware sample known as Cobalt Strike. This strike sends a malware sample known as a Cobalt Strike PowerShell loader. This malware is a PowerShell-based loader that decrypts and executes shellcode directly in memory to deliver a Cobalt Strike Beacon. It is distributed through a publicly accessible .ps1 script hosted on infrastructure associated with Chinese and Russian regions. The loader employs evasion techniques such as API hashing, dynamic function resolution, and forged User-Agent headers. It retrieves its second-stage payload from a Baidu Cloud Function endpoint and communicates with a Russian-hosted command and control server using a Cobalt Strike SSL certificate. The MD5 hash of this Cobalt Strike sample is 7e9fe1a831d4c4714d16c7ec39f79b5d.</p>

<b>Name</b>	<b>Description</b>
Strike CobaltStrike_9dc0a907	<p>This strike sends a malware sample known as Cobalt Strike. This strike sends a malware sample known as a Cobalt Strike PowerShell loader. This malware is a PowerShell-based loader that decrypts and executes shellcode directly in memory to deliver a Cobalt Strike Beacon. It is distributed through a publicly accessible .ps1 script hosted on infrastructure associated with Chinese and Russian regions. The loader employs evasion techniques such as API hashing, dynamic function resolution, and forged User-Agent headers. It retrieves its second-stage payload from a Baidu Cloud Function endpoint and communicates with a Russian-hosted command and control server using a Cobalt Strike SSL certificate. The MD5 hash of this Cobalt Strike sample is 9dc0a907c4136946f8d3b0c42ebf677f.</p>
Strike CobaltStrike_a24d1503	<p>This strike sends a malware sample known as Cobalt Strike. This strike sends a malware sample known as a Cobalt Strike PowerShell loader. This malware is a PowerShell-based loader that decrypts and executes shellcode directly in memory to deliver a Cobalt Strike Beacon. It is distributed through a publicly accessible .ps1 script hosted on infrastructure associated with Chinese and Russian regions. The loader employs evasion techniques such as API hashing, dynamic function resolution, and forged User-Agent headers. It retrieves its second-stage payload from a Baidu Cloud Function endpoint and communicates with a Russian-hosted command and control server using a Cobalt Strike SSL certificate. The MD5 hash of this Cobalt Strike sample is a24d1503a25ba3f8bbe6348ad7d5a553.</p>
Strike CobaltStrike_af3ff304	<p>This strike sends a malware sample known as Cobalt Strike. This strike sends a malware sample known as a Cobalt Strike PowerShell loader. This malware is a PowerShell-based loader that decrypts and executes shellcode directly in memory to deliver a Cobalt Strike Beacon. It is distributed through a publicly accessible .ps1 script hosted on infrastructure associated with Chinese and Russian regions. The loader employs evasion techniques such as API hashing, dynamic function resolution, and forged User-Agent headers. It retrieves its second-stage payload from a Baidu Cloud Function endpoint and communicates with a Russian-hosted command and control server using a Cobalt Strike SSL certificate. The MD5 hash of this Cobalt Strike sample is af3ff304eb1892e8890e0b57ba78355a.</p>
Strike CobaltStrike_c5827727	<p>This strike sends a malware sample known as Cobalt Strike. This strike sends a malware sample known as a Cobalt Strike PowerShell loader. This malware is a PowerShell-based loader that decrypts and executes shellcode directly in memory to deliver a Cobalt Strike Beacon. It is distributed through a publicly accessible .ps1 script hosted on infrastructure associated with Chinese and Russian regions. The loader employs evasion techniques such as API hashing, dynamic function resolution, and forged User-Agent headers. It retrieves its second-stage payload from a Baidu Cloud Function endpoint and communicates with a Russian-hosted command and control server using a Cobalt Strike SSL certificate. The MD5 hash of this Cobalt Strike sample is c58277271a558ebafdf06da61dc074bf4.</p>

Name	Description
Strike CobaltStrike_ccff29e6	This strike sends a malware sample known as Cobalt Strike. This strike sends a malware sample known as a Cobalt Strike PowerShell loader. This malware is a PowerShell-based loader that decrypts and executes shellcode directly in memory to deliver a Cobalt Strike Beacon. It is distributed through a publicly accessible .ps1 script hosted on infrastructure associated with Chinese and Russian regions. The loader employs evasion techniques such as API hashing, dynamic function resolution, and forged User-Agent headers. It retrieves its second-stage payload from a Baidu Cloud Function endpoint and communicates with a Russian-hosted command and control server using a Cobalt Strike SSL certificate. The MD5 hash of this Cobalt Strike sample is ccff29e656e293a5240925a38a7dd173.
Strike CobaltStrike_da15e8aa	This strike sends a malware sample known as Cobalt Strike. This strike sends a malware sample known as a Cobalt Strike PowerShell loader. This malware is a PowerShell-based loader that decrypts and executes shellcode directly in memory to deliver a Cobalt Strike Beacon. It is distributed through a publicly accessible .ps1 script hosted on infrastructure associated with Chinese and Russian regions. The loader employs evasion techniques such as API hashing, dynamic function resolution, and forged User-Agent headers. It retrieves its second-stage payload from a Baidu Cloud Function endpoint and communicates with a Russian-hosted command and control server using a Cobalt Strike SSL certificate. The MD5 hash of this Cobalt Strike sample is da15e8aa592ad3fd7a43bba187a4a706.
Strike Conti_290c7dfb	This strike sends a malware sample known as Conti. Conti is a Ransomware-as-a-Service, that in the past has been associated with TrickBot, and is being called the successor to Ryuk. Most recently it has been seen attacking large organizations and government agencies. Conti not only encrypts the victim's files, but also steals their data and threatens to publish the stolen data. It uses known vulnerabilities like in Microsoft SMB and MS Print Spooler CVE-2021-34527 to escalate privileges and move laterally throughout the network. Conti deploys Cobalt Strike beacons to perform C2 functionality, but also installs remote management software like AnyDesk and Atera to maintain persistence. The MD5 hash of this Conti sample is 290c7dfb01e50cea9e19da81a781af2c.
Strike Conti_50e767c6	This strike sends a malware sample known as Conti. Conti is a Ransomware-as-a-Service, that in the past has been associated with TrickBot, and is being called the successor to Ryuk. Most recently it has been seen attacking large organizations and government agencies. Conti not only encrypts the victim's files, but also steals their data and threatens to publish the stolen data. It uses known vulnerabilities like in Microsoft SMB and MS Print Spooler CVE-2021-34527 to escalate privileges and move laterally throughout the network. Conti deploys Cobalt Strike beacons to perform C2 functionality, but also installs remote management software like AnyDesk and Atera to maintain persistence. The MD5 hash of this Conti sample is 50e767c614b48b05c6d6574edfcacb2a.

<b>Name</b>	<b>Description</b>
Strike Conti_617ccca7	This strike sends a malware sample known as Conti. Conti is a Ransomware-as-a-Service, that in the past has been associated with TrickBot, and is being called the successor to Ryuk. Most recently it has been seen attacking large organizations and government agencies. Conti not only encrypts the victim's files, but also steals their data and threatens to publish the stolen data. It uses known vulnerabilities like in Microsoft SMB and MS Print Spooler CVE-2021-34527 to escalate privileges and move laterally throughout the network. Conti deploys Cobalt Strike beacons to perform C2 functionality, but also installs remote management software like AnyDesk and Atera to maintain persistence. The MD5 hash of this Conti sample is 617ccca7d5753993cbfd1309d1a18e1c.
Strike Conti_90c44980	This strike sends a malware sample known as Conti. Conti is a Ransomware-as-a-Service, that in the past has been associated with TrickBot, and is being called the successor to Ryuk. Most recently it has been seen attacking large organizations and government agencies. Conti not only encrypts the victim's files, but also steals their data and threatens to publish the stolen data. It uses known vulnerabilities like in Microsoft SMB and MS Print Spooler CVE-2021-34527 to escalate privileges and move laterally throughout the network. Conti deploys Cobalt Strike beacons to perform C2 functionality, but also installs remote management software like AnyDesk and Atera to maintain persistence. The MD5 hash of this Conti sample is 90c449800919d3905466e7baf739ad6d.
Strike Conti_9152cb45	This strike sends a malware sample known as Conti. Conti is a Ransomware-as-a-Service, that in the past has been associated with TrickBot, and is being called the successor to Ryuk. Most recently it has been seen attacking large organizations and government agencies. Conti not only encrypts the victim's files, but also steals their data and threatens to publish the stolen data. It uses known vulnerabilities like in Microsoft SMB and MS Print Spooler CVE-2021-34527 to escalate privileges and move laterally throughout the network. Conti deploys Cobalt Strike beacons to perform C2 functionality, but also installs remote management software like AnyDesk and Atera to maintain persistence. The MD5 hash of this Conti sample is 9152cb45994adab4dc27c33ee72a66e1.
Strike Conti_d7bf01f9	This strike sends a malware sample known as Conti. Conti is a Ransomware-as-a-Service, that in the past has been associated with TrickBot, and is being called the successor to Ryuk. Most recently it has been seen attacking large organizations and government agencies. Conti not only encrypts the victim's files, but also steals their data and threatens to publish the stolen data. It uses known vulnerabilities like in Microsoft SMB and MS Print Spooler CVE-2021-34527 to escalate privileges and move laterally throughout the network. Conti deploys Cobalt Strike beacons to perform C2 functionality, but also installs remote management software like AnyDesk and Atera to maintain persistence. The MD5 hash of this Conti sample is d7bf01f9fb24176f2d42d770d79e8c2c.
Strike Conti_e099a53f	This strike sends a malware sample known as Conti. Conti is a Ransomware-as-a-Service, that in the past has been associated with TrickBot, and is being called the successor to Ryuk. Most recently it has been seen attacking large organizations and government agencies. Conti not only encrypts the victim's files, but also steals their data and threatens to publish the stolen data. It uses known vulnerabilities like in Microsoft SMB and MS Print Spooler CVE-2021-34527 to escalate privileges and move laterally throughout the network. Conti deploys Cobalt Strike beacons to perform C2 functionality, but also installs remote management software like AnyDesk and Atera to maintain persistence. The MD5 hash of this Conti sample is e099a53fdcef7bdfb58b3a7b4f42e4d2.

<b>Name</b>	<b>Description</b>
Strike Copybara_03ee48f6	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 03ee48f6e7f0840ef94336af579ccdf4.
Strike Copybara_0596663c	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 0596663c542e7cfb4473c8c8ef86eee5.
Strike Copybara_112bc421	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 112bc421690788f883e62742cd7e142a.
Strike Copybara_1150d0bf	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 1150d0bf3a077be4f33eb487129d389a.
Strike Copybara_14e70653	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 14e70653b82895367d33ec8570c9038e.
Strike Copybara_18ac895a	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 18ac895a5f348d2a05d6a07a213d84a6.
Strike Copybara_1ec0f869	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 1ec0f8696578e0e427140fd256ec4e4f.
Strike Copybara_215ca929	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 215ca929eea5866ef9e879fe37f9ce17.
Strike Copybara_215eb7fd	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 215eb7fd4c261e17a696e8ba6a4061ed.

<b>Name</b>	<b>Description</b>
Strike Copybara_22483da7	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 22483da70e998a316e9ac5b905b0fc9e.
Strike Copybara_271f79eb	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 271f79eb4ca49040fef16725777ac577.
Strike Copybara_28f2aaa7	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 28f2aaa7855c1a2d5e5ec6444fa833a9.
Strike Copybara_2c36088f	This strike sends a malware sample known as Copybara. It is an Android malware spread through vishing attacks and masquerades as legitimate financial apps. It exploits the Accessibility Service to control infected devices, downloading phishing pages that impersonate cryptocurrency exchanges and financial institutions. The malware steals credentials and performs keylogging, SMS interception, screen capturing, and remote device control. It leverages the MQTT protocol for efficient communication with its C2 server. 'com.sastiupana.newicon' is the package name of the malware sample. The MD5 hash of this malware sample is 2c36088fec061815bdcebb93aec8771d.
Strike Copybara_2d04f0f8	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 2d04f0f898b452f05521a71ee2457eab.
Strike Copybara_304f779e	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 304f779e21b4f70f4ce70ce4dd19dbe8.
Strike Copybara_3251cb47	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 3251cb4712b6c7aeb3f48c3ef767c735.
Strike Copybara_3c90ca08	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 3c90ca08d834d4650409a4282bbe6d42.

<b>Name</b>	<b>Description</b>
Strike Copybara_3eaafdc6	This strike sends a polymorphic malware sample known as Copybara. It is an Android malware spread through vishing attacks and masquerades as legitimate financial apps. It exploits the Accessibility Service to control infected devices, downloading phishing pages that impersonate cryptocurrency exchanges and financial institutions. The malware steals credentials and performs keylogging, SMS interception, screen capturing, and remote device control. It leverages the MQTT protocol for efficient communication with its C2 server. 'com.sastiupana.newicon' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this Copybara sample is 3eaafdc602ab53fa199bc797970f0cb7.
Strike Copybara_459b8182	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is 459b8182aaaf3ef14e9fd4754b40610a.
Strike Copybara_45b6c878	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is 45b6c878e32dafc7fd16f9c088637be2.
Strike Copybara_4637f70b	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is 4637f70bb727b40f3d7e8be88da1f244.
Strike Copybara_47cf4564	This strike sends a polymorphic malware sample known as Copybara. It is an Android malware spread through vishing attacks and masquerades as legitimate financial apps. It exploits the Accessibility Service to control infected devices, downloading phishing pages that impersonate cryptocurrency exchanges and financial institutions. The malware steals credentials and performs keylogging, SMS interception, screen capturing, and remote device control. It leverages the MQTT protocol for efficient communication with its C2 server. 'com.intesatoken.appnuova' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this Copybara sample is 47cf4564ddf329f97ba929c302f36682.
Strike Copybara_4e519739	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is 4e51973921f1bf1c26b7d045d9716ae8.
Strike Copybara_4f007c67	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is 4f007c674721466ff8af2d6b8b0e6040.

<b>Name</b>	<b>Description</b>
Strike Copybara_5391b950	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 5391b95013437f299b6d096ad2fc96fb.
Strike Copybara_53be8d45	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 53be8d45faa3f943faf51fc95b76df5b.
Strike Copybara_5bfe70c2	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 5bfe70c2ab56c92e88563885294c0fa7.
Strike Copybara_5f0ce16f	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 5f0ce16fd6fe97db0aad3ccf70c5da82.
Strike Copybara_63890a15	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 63890a15099a0debd9ed2a3b2036c956.
Strike Copybara_65040bd2	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 65040bd2de9805826d66d1ff5996ed52.
Strike Copybara_67664abf	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 67664abfaec4d2d7e387c988d0c003ca.
Strike Copybara_68c7a979	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 68c7a9796ef7c50c56513618b6ab4f9c.
Strike Copybara_6d8af62f	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 6d8aff62f295ac4fcf23d20af97339440.

<b>Name</b>	<b>Description</b>
Strike Copybara_6eb2123c	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 6eb2123c58bb283790a43b5fdaf1c25.
Strike Copybara_6f2d9627	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 6f2d962721f731fb53abeb53da0cabbc2.
Strike Copybara_71896aa3	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 71896aa37e39028680b628cb05080028.
Strike Copybara_71c85d6f	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 71c85d6fabe4573403f5597d616daa41.
Strike Copybara_7a4e9e56	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 7a4e9e5692e0031e130dbc41f3d74b82.
Strike Copybara_7c203ad3	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 7c203ad3d565fce177adf272d0acd373.
Strike Copybara_7e7edf3b	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 7e7edf3b1f5f0f4bdc77af7a3a5e34c5.
Strike Copybara_88956e2b	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 88956e2b3ca08e5759a8bf279bf49345.

<b>Name</b>	<b>Description</b>
Strike Copybara_906fa151	This strike sends a polymorphic malware sample known as Copybara. It is an Android malware spread through phishing attacks and masquerades as legitimate financial apps. It exploits the Accessibility Service to control infected devices, downloading phishing pages that impersonate cryptocurrency exchanges and financial institutions. The malware steals credentials and performs keylogging, SMS interception, screen capturing, and remote device control. It leverages the MQTT protocol for efficient communication with its C2 server. 'com.sastiupana.newicon' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this Copybara sample is 906fa15197836c0c5ef104111fb25e62.
Strike Copybara_933a030b	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is 933a030b3d7559a41a406f52a006c30f.
Strike Copybara_93d05bac	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is 93d05bac003f669b8d0cb9d0ac23a705.
Strike Copybara_93e4313e	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is 93e4313edc3e70c4e50c418f1f44be80.
Strike Copybara_952af76a	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is 952af76aea0773021cfb1932245a3711.
Strike Copybara_99c2d958	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is 99c2d9582ecc4a34e466cf71e6054e84.
Strike Copybara_99eee5c0	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is 99eee5c0856271604905dfc66fc03fca.
Strike Copybara_9aa6f175	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is 9aa6f175b7520878ecffe98444c1b336.

<b>Name</b>	<b>Description</b>
Strike Copybara_9be33294	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 9be332949fff5d1c9492c2c93f12aced.
Strike Copybara_9f2e8bcc	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 9f2e8bcc93740b9fc8122ad7abcc43c9.
Strike Copybara_9f904c5a	This strike sends a polymorphic malware sample known as Copybara. It is an Android malware spread through vishing attacks and masquerades as legitimate financial apps. It exploits the Accessibility Service to control infected devices, downloading phishing pages that impersonate cryptocurrency exchanges and financial institutions. The malware steals credentials and performs keylogging, SMS interception, screen capturing, and remote device control. It leverages the MQTT protocol for efficient communication with its C2 server. 'com.intesatoken.appnuova' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this Copybara sample is 9f904c5a442d8efe06818c277307b11d.
Strike Copybara_9f9b4a2a	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is 9f9b4a2a21cf2be7e62db08beae733c3.
Strike Copybara_a1f36b2a	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is a1f36b2ada4b63b50eeb482777b44e90.
Strike Copybara_a57e009f	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is a57e009fdee84765642e655e4802c288.
Strike Copybara_a5ec70b5	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is a5ec70b5430309ea5d9ca1b5aa55c532.
Strike Copybara_a6c4e84b	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is a6c4e84be479e5ec13656491b485cf19.

<b>Name</b>	<b>Description</b>
Strike Copybara_a9036e85	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is a9036e8521431d6f6d50ea31ccdee96d.
Strike Copybara_a95315ca	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is a95315ca7af6d857379adb2c87f27c72.
Strike Copybara_af869a4a	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is af869a4ab0bf10e528b0190a721cd7fc.
Strike Copybara_b0cc816a	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is b0cc816ac58ef4e309aab3362dc6b8ab.
Strike Copybara_b1109bd8	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is b1109bd86eed5b4badd2eaf099c65f9.
Strike Copybara_b3f067b4	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is b3f067b4dfea589351b3f5f25dfb1b3c.
Strike Copybara_b4b85702	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is b4b85702d206534735f85b783123dc1a.
Strike Copybara_ba1c2891	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is ba1c2891d626401c5e1eb5b677ef2804.

Name	Description
Strike Copybara_bb2d3c26	This strike sends a malware sample known as Copybara. It is an Android malware spread through vishing attacks and masquerades as legitimate financial apps. It exploits the Accessibility Service to control infected devices, downloading phishing pages that impersonate cryptocurrency exchanges and financial institutions. The malware steals credentials and performs keylogging, SMS interception, screen capturing, and remote device control. It leverages the MQTT protocol for efficient communication with its C2 server. 'com.intesatoken.appnuova' is the package name of the malware sample. The MD5 hash of this Copybara sample is bb2d3c26762eaa3b9c0bc1915dfe8ca0.
Strike Copybara_bf8fe1d0	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is bf8fe1d0e877a1f232cd1c4bf945c866.
Strike Copybara_c4ef1662	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is c4ef1662adb4c441b9eed950adcfe820.
Strike Copybara_cb8e75a3	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is cb8e75a3d907ad22eec1bacafce09265.
Strike Copybara_cd92e893	This strike sends a polymorphic malware sample known as Copybara. It is an Android malware spread through vishing attacks and masquerades as legitimate financial apps. It exploits the Accessibility Service to control infected devices, downloading phishing pages that impersonate cryptocurrency exchanges and financial institutions. The malware steals credentials and performs keylogging, SMS interception, screen capturing, and remote device control. It leverages the MQTT protocol for efficient communication with its C2 server. 'com.sastiupana.newicon' is the package name of the malware sample. Constant strings in the code has been encrypted. The MD5 hash of this Copybara sample is cd92e893e4fc5aee975daed0fd8e7b7a.
Strike Copybara_d55ee912	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is d55ee912c682c9c6aecec279681c6443.
Strike Copybara_d5b765f4	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is d5b765f43eb431f3a4b8e49905282843.

<b>Name</b>	<b>Description</b>
Strike Copybara_e1e54169	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is e1e541699986840a6548407df21086d6.
Strike Copybara_e3206520	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is e3206520c98f993d5a3096fa88fe5ebb.
Strike Copybara_e6e4cc18	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is e6e4cc18665a2cc546979499224241cd.
Strike Copybara_e9eede20	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is e9eede200e5735e60a01bde6d4bf5a54.
Strike Copybara_eaff7697	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is eaff7697d0bc139cd3f2c2527522982e.
Strike Copybara_ed9c745a	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is ed9c745a566fc35e7f24e6b70bbb57cf.
Strike Copybara_f0ffd34	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is f0ffd3459637546cff65cff79da1bde7.
Strike Copybara_f1ae4692	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is f1ae4692dfd5977fdec487bf55119008.
Strike Copybara_f2bc8d8c	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server The MD5 hash of this Copybara sample is f2bc8d8c94dc9e195c90060c1642c938.

<b>Name</b>	<b>Description</b>
Strike Copybara_f54c526d	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is f54c526d2937c59a44577fdb9852e793.
Strike Copybara_f78d9480	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is f78d948076546bc7ea814e8a68ea47cf.
Strike Copybara_fabf4131	This strike sends a polymorphic malware sample known as Copybara. It is an Android malware spread through vishing attacks and masquerades as legitimate financial apps. It exploits the Accessibility Service to control infected devices, downloading phishing pages that impersonate cryptocurrency exchanges and financial institutions. The malware steals credentials and performs keylogging, SMS interception, screen capturing, and remote device control. It leverages the MQTT protocol for efficient communication with its C2 server. 'com.intesatoken.appnuova' is the package name of the malware sample. Constant strings in the code has been encrypted. The MD5 hash of this Copybara sample is fabf41317034f05724b6c11d80f8ebf8.
Strike Copybara_ff0a3bd9	This strike sends a malware sample known as Copybara. Copybara is an Android trojan. It includes many capabilities like keylogging, multimedia recording, screen capturing, and remote device control. Copybara uses MQTT to communicate with the attacker C2 server. The MD5 hash of this Copybara sample is ff0a3bd90f9f7359540d8759af3f2c99.
Strike CoralRaider_118ff6bf	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is 118ff6bf510b61c6a4e7a11b465bdbaa.
Strike CoralRaider_1c802d77	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is 1c802d7721f354b57e4a0e28788a7278.
Strike CoralRaider_231e8c4e	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is 231e8c4e5bef8e8a1e352dbb7c97100d.

<b>Name</b>	<b>Description</b>
Strike CoralRaider_2f6afa2f	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is 2f6afa2fcc7047a5cc92f193945c9ae2.
Strike CoralRaider_309c2e58	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is 309c2e58a60117b1943731995a49c06c.
Strike CoralRaider_3e48f80c	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is 3e48f80c959a5c47854e260cb975a6dd.
Strike CoralRaider_57965340	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is 57965340966b56befcc24e6c11b5afdf.
Strike CoralRaider_6927beab	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is 6927beab231d254cdc66fc8004c76fd.
Strike CoralRaider_7c1d3d83	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is 7c1d3d83db6393781e5d35972273720d.
Strike CoralRaider_83fac34f	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is 83fac34f21d0a9addefc653c68d63463.

Name	Description
Strike CoralRaider_8527635e	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is 8527635ef61d35dc68350c97374cf4f2.
Strike CoralRaider_862c45dc	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is 862c45dca475a210fa65c26a0e38c88c.
Strike CoralRaider_ab1d3e72	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is ab1d3e723949526483c90ca2e0f0f1f6.
Strike CoralRaider_bfa936de	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is bfa936de26037dd4693af0f8d69cddc8.
Strike CoralRaider_ca5e9fed	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is ca5e9fed7743c871358c9f29bb477947.
Strike CoralRaider_ce5fb5a	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is ce5fb5af0805ae714563ea936298358.
Strike CoralRaider_d25195da	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is d25195dac69807fe69ce9e00bfeee71a.

<b>Name</b>	<b>Description</b>
Strike CoralRaider_f0c732dd	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is f0c732dd166146b17a048b2655d5ff75.
Strike CoralRaider_f1bcaab5	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is f1bcaab51a0b18e531cdac76909f4541.
Strike CoralRaider_f75e029c	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is f75e029c90ba91bd8c456ce08a8b5ed5.
Strike CoralRaider_fa23d314	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is fa23d314aad9190927e56831e506c3ee.
Strike CoralRaider_ff93e477	This strike sends a malware sample known as CoralRaider. This malware sample is associated with the CoralRaider threat actor and has been seen in a campaign in which a Windows shortcut file to execute an HTA file on a remotely hosted machine. This HTA file executes an embedded Windows Powershell decrypter that eventually downloads and executes one of the following malicious payloads CryptBot, LummaC2 or Rhadamanthys. The MD5 hash of this CoralRaider sample is ff93e4776d6131a014e96421a7df26ab.
Strike CriminalMW_2cfcdc58	This strike sends a polymorphic malware sample known as CriminalMW. CriminalMW, also known as GoatRAT and FantasyMW, is an Android banking trojan malware classified as a Remote Access Trojan (RAT). The malware primarily targets Brazilian banks, aiming to steal financial information. It can steal various sensitive pieces of information from the infected device, including messages, call logs, and photographs. Attackers can remotely control the device, allowing them to perform actions such as taking screenshots, recording audio and video, and executing commands. CriminalMW employs anti-emulation techniques to evade detection by security software. 'biz.uea.xgn' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 2cfcdc58e77faa2717f13bd91153509c.

<b>Name</b>	<b>Description</b>
Strike CriminalMW_30b7d1c8	<p>This strike sends a malware sample known as CriminalMW. CriminalMW, also known as GoatRAT and FantasyMW, is an Android banking trojan malware classified as a Remote Access Trojan (RAT). The malware primarily targets Brazilian banks, aiming to steal financial information. It can steal various sensitive pieces of information from the infected device, including messages, call logs, and photographs. Attackers can remotely control the device, allowing them to perform actions such as taking screenshots, recording audio and video, and executing commands. CriminalMW employs anti-emulation techniques to evade detection by security software. 'biz.uea.xgn' is the package name of the malware sample. The MD5 hash of this malware sample is 30b7d1c865335266979e96f8ddfb708.</p>
Strike CriminalMW_30f1be89	<p>This strike sends a malware sample known as CriminalMW. CriminalMW, also known as GoatRAT and FantasyMW, is an Android banking trojan malware classified as a Remote Access Trojan (RAT). The malware primarily targets Brazilian banks, aiming to steal financial information. It can steal various sensitive pieces of information from the infected device, including messages, call logs, and photographs. Attackers can remotely control the device, allowing them to perform actions such as taking screenshots, recording audio and video, and executing commands. CriminalMW employs anti-emulation techniques to evade detection by security software. 'com.dzw.imc' is the package name of the malware sample. The MD5 hash of this malware sample is 30f1be8974e018e6b293fe5de9515bcc.</p>
Strike CriminalMW_53a3824f	<p>This strike sends a polymorphic malware sample known as CriminalMW. CriminalMW, also known as GoatRAT and FantasyMW, is an Android banking trojan malware classified as a Remote Access Trojan (RAT). The malware primarily targets Brazilian banks, aiming to steal financial information. It can steal various sensitive pieces of information from the infected device, including messages, call logs, and photographs. Attackers can remotely control the device, allowing them to perform actions such as taking screenshots, recording audio and video, and executing commands. CriminalMW employs anti-emulation techniques to evade detection by security software. 'biz.uea.xgn' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 53a3824fce8fe0bbcd03ad938120a62b.</p>
Strike CriminalMW_5789dd8c	<p>This strike sends a polymorphic malware sample known as CriminalMW. CriminalMW, also known as GoatRAT and FantasyMW, is an Android banking trojan malware classified as a Remote Access Trojan (RAT). The malware primarily targets Brazilian banks, aiming to steal financial information. It can steal various sensitive pieces of information from the infected device, including messages, call logs, and photographs. Attackers can remotely control the device, allowing them to perform actions such as taking screenshots, recording audio and video, and executing commands. CriminalMW employs anti-emulation techniques to evade detection by security software. 'biz.uea.xgn' is the package name of the malware sample. Constant strings in the code has been encrypted. The MD5 hash of this malware sample is 5789dd8c121d6d30a71937935d08004a.</p>

Name	Description
Strike CriminalMW_e68b88b6	This strike sends a polymorphic malware sample known as CriminalMW. CriminalMW, also known as GoatRAT and FantasyMW, is an Android banking trojan malware classified as a Remote Access Trojan (RAT). The malware primarily targets Brazilian banks, aiming to steal financial information. It can steal various sensitive pieces of information from the infected device, including messages, call logs, and photographs. Attackers can remotely control the device, allowing them to perform actions such as taking screenshots, recording audio and video, and executing commands. CriminalMW employs anti-emulation techniques to evade detection by security software. 'com.dzw.imc' is the package name of the malware sample. Constant strings in the code have been encrypted. The MD5 hash of this malware sample is e68b88b63a44285a7d3899d1b076d703.
Strike CriminalMW_ef41354a	This strike sends a polymorphic malware sample known as CriminalMW. CriminalMW, also known as GoatRAT and FantasyMW, is an Android banking trojan malware classified as a Remote Access Trojan (RAT). The malware primarily targets Brazilian banks, aiming to steal financial information. It can steal various sensitive pieces of information from the infected device, including messages, call logs, and photographs. Attackers can remotely control the device, allowing them to perform actions such as taking screenshots, recording audio and video, and executing commands. CriminalMW employs anti-emulation techniques to evade detection by security software. 'com.dzw.imc' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is ef41354a2f1a3b1c660a180940812bb3.
Strike CriminalMW_fb667c93	This strike sends a polymorphic malware sample known as CriminalMW. CriminalMW, also known as GoatRAT and FantasyMW, is an Android banking trojan malware classified as a Remote Access Trojan (RAT). The malware primarily targets Brazilian banks, aiming to steal financial information. It can steal various sensitive pieces of information from the infected device, including messages, call logs, and photographs. Attackers can remotely control the device, allowing them to perform actions such as taking screenshots, recording audio and video, and executing commands. CriminalMW employs anti-emulation techniques to evade detection by security software. 'com.dzw.imc' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is fb667c934f4b655e635b63227d136289.
Strike CrossLock_9756b1c7	This strike sends a malware sample known as CrossLock. CrossLock is ransomware that is written in the GoLang programming language. It encrypts the victim's data as well as exfiltrates it. If the ransom is not paid the attackers threaten to leak the stolen information. The MD5 hash of this CrossLock sample is 9756b1c7d0001100fdde3efefb7e086f.
Strike Cuckoo_11621569	This strike sends a malware sample known as Cuckoo. Cuckoo is a variant of the malware AMOS or Atomic macOS Stealer. This deployment of this malware occurs after a user visits a malicious Homebrew site that requires the user to execute a download command in the terminal similar to the legitimate Homebrew webpage. The malware gathers lots of information including wallets, passwords, other sensitive data, and then exfiltrates it back to the attacker. It also includes anti Virtual Machine Analysis capabilities. The MD5 hash of this Cuckoo sample is 116215690d7a5bdffe0ac911a36fb765.

<b>Name</b>	<b>Description</b>
Strike Cuckoo_269b1937	This strike sends a malware sample known as Cuckoo. Cuckoo is variant of the malware AMOS or Atomic macOS Stealer. This deployment of this malware occurs after a user visits a malicious Homebrew site that requires the user to execute a download command in the terminal similar to the legitimate Homebrew webpage. The malware gathers lots of information including wallets, passwords, other sensitive data, and then exfiltrates it back to the attacker. It also includes anti Virtual Machine Analysis capabilities. The MD5 hash of this Cuckoo sample is 269b193738b0eca54147338211719478.
Strike Cuckoo_48e8393d	This strike sends a malware sample known as Cuckoo. Cuckoo is variant of the malware AMOS or Atomic macOS Stealer. This deployment of this malware occurs after a user visits a malicious Homebrew site that requires the user to execute a download command in the terminal similar to the legitimate Homebrew webpage. The malware gathers lots of information including wallets, passwords, other sensitive data, and then exfiltrates it back to the attacker. It also includes anti Virtual Machine Analysis capabilities. The MD5 hash of this Cuckoo sample is 48e8393d54d8eb4827961dbb6020c07c.
Strike Cuckoo_6f57b6a1	This strike sends a malware sample known as Cuckoo. Cuckoo is variant of the malware AMOS or Atomic macOS Stealer. This deployment of this malware occurs after a user visits a malicious Homebrew site that requires the user to execute a download command in the terminal similar to the legitimate Homebrew webpage. The malware gathers lots of information including wallets, passwords, other sensitive data, and then exfiltrates it back to the attacker. It also includes anti Virtual Machine Analysis capabilities. The MD5 hash of this Cuckoo sample is 6f57b6a1e6cfbc3cd46888723ffb0104.
Strike Cuckoo_8ac7c634	This strike sends a malware sample known as Cuckoo. Cuckoo is variant of the malware AMOS or Atomic macOS Stealer. This deployment of this malware occurs after a user visits a malicious Homebrew site that requires the user to execute a download command in the terminal similar to the legitimate Homebrew webpage. The malware gathers lots of information including wallets, passwords, other sensitive data, and then exfiltrates it back to the attacker. It also includes anti Virtual Machine Analysis capabilities. The MD5 hash of this Cuckoo sample is 8ac7c6345bc5ce088409ddc4836e5b89.
Strike Cuckoo_ad0dc846	This strike sends a malware sample known as Cuckoo. Cuckoo is variant of the malware AMOS or Atomic macOS Stealer. This deployment of this malware occurs after a user visits a malicious Homebrew site that requires the user to execute a download command in the terminal similar to the legitimate Homebrew webpage. The malware gathers lots of information including wallets, passwords, other sensitive data, and then exfiltrates it back to the attacker. It also includes anti Virtual Machine Analysis capabilities. The MD5 hash of this Cuckoo sample is ad0dc84634906434e571681d901056d3.

<b>Name</b>	<b>Description</b>
Strike Cuckoo_cad2cd91	This strike sends a malware sample known as Cuckoo. Cuckoo is variant of the malware AMOS or Atomic macOS Stealer. This deployment of this malware occurs after a user visits a malicious Homebrew site that requires the user to execute a download command in the terminal similar to the legitimate Homebrew webpage. The malware gathers lots of information including wallets, passwords, other sensitive data, and then exfiltrates it back to the attacker. It also includes anti Virtual Machine Analysis capabilities. The MD5 hash of this Cuckoo sample is cad2cd91df26c92ecf246c01276f6c2f.
Strike Cuckoo_d66c04ef	This strike sends a malware sample known as Cuckoo. Cuckoo is variant of the malware AMOS or Atomic macOS Stealer. This deployment of this malware occurs after a user visits a malicious Homebrew site that requires the user to execute a download command in the terminal similar to the legitimate Homebrew webpage. The malware gathers lots of information including wallets, passwords, other sensitive data, and then exfiltrates it back to the attacker. It also includes anti Virtual Machine Analysis capabilities. The MD5 hash of this Cuckoo sample is d66c04ef314b3a43f011f681324b256c.
Strike CyberVolk_35815ae7	This strike sends a malware sample known as CyberVolk. CyberVolk is a Russian aligned group that utilizes malware against targets that have opposing interests to Russia. This malware is ransomware that scans and encrypts files and demands payment via Bitcoin. The MD5 hash of this CyberVolk sample is 35815ae7affca262bcd6beabbdadebfd.
Strike CyberVolk_38fb9ac2	This strike sends a malware sample known as CyberVolk. CyberVolk is a Russian aligned group that utilizes malware against targets that have opposing interests to Russia. This malware is ransomware that scans and encrypts files and demands payment via Bitcoin. The MD5 hash of this CyberVolk sample is 38fb9ac2e51d04182faf81afbef08ab8.
Strike CyberVolk_4e66429d	This strike sends a malware sample known as CyberVolk. CyberVolk is a Russian aligned group that utilizes malware against targets that have opposing interests to Russia. This malware is ransomware that scans and encrypts files and demands payment via Bitcoin. The MD5 hash of this CyberVolk sample is 4e66429d85967e344d8354e9b81719dc.
Strike CyberVolk_535bc51f	This strike sends a malware sample known as CyberVolk. CyberVolk is a Russian aligned group that utilizes malware against targets that have opposing interests to Russia. This malware is ransomware that scans and encrypts files and demands payment via Bitcoin. The MD5 hash of this CyberVolk sample is 535bc51f49d1106cf06dfe92ad0444b5.
Strike CyberVolk_57e7e215	This strike sends a malware sample known as CyberVolk. CyberVolk is a Russian aligned group that utilizes malware against targets that have opposing interests to Russia. This malware is ransomware that scans and encrypts files and demands payment via Bitcoin. The MD5 hash of this CyberVolk sample is 57e7e2151ac4443d3a30d61d4426428a.
Strike CyberVolk_626fab82	This strike sends a malware sample known as CyberVolk. CyberVolk is a Russian aligned group that utilizes malware against targets that have opposing interests to Russia. This malware is ransomware that scans and encrypts files and demands payment via Bitcoin. The MD5 hash of this CyberVolk sample is 626fab8275d8d8e841bc9a08b208201e.

<b>Name</b>	<b>Description</b>
Strike CyberVolk_648bd793	This strike sends a malware sample known as CyberVolk. CyberVolk is a Russian aligned group that utilizes malware against targets that have opposing interests to Russia. This malware is ransomware that scans and encrypts files and demands payment via Bitcoin. The MD5 hash of this CyberVolk sample is 648bd793d9e54fc2741e0ba10980c7de.
Strike CyberVolk_889e6365	This strike sends a malware sample known as CyberVolk. CyberVolk is a Russian aligned group that utilizes malware against targets that have opposing interests to Russia. This malware is ransomware that scans and encrypts files and demands payment via Bitcoin. The MD5 hash of this CyberVolk sample is 889e6365d82a9a89b6c8c86d672b8f0c.
Strike DOGcall_394e52e2	This strike sends a malware sample known as DOGcall. DOGcall aslo known as ROKRat is a family of malware that was initially seen from attackers originating from North Korea. The malware has a loader that drops the core payload. This sample is the final payload, and it is a Remote Access Trojan that provides the attacker with a number of functions including data exfiltration, credential harvesting, screenshots of the system, and communicating with a remote C2 server for additional received commands. The MD5 hash of this DOGcall sample is 394e52e219feb1a5c403714154048728.
Strike DOGcall_dc6c2033	This strike sends a polymorphic malware sample known as DOGcall. DOGcall aslo known as ROKRat is a family of malware that was initially seen from attackers originating from North Korea. The malware has a loader that drops the core payload. This sample is the final payload, and it is a Remote Access Trojan that provides the attacker with a number of functions including data exfiltration, credential harvesting, screenshots of the system, and communicating with a remote C2 server for additional received commands. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this DOGcall sample is dc6c20333f94a04c6cdea4fe9211ac09.
Strike DUSTPAN_17d0ada8	This strike sends a malware sample known as DUSTPAN. DUSTPAN is a in-memory dropper that decrypts and executes an embedded payload. It has been associated with the Chinese state-sponsored cyber threat group APT41, and has been tied to many different sectors like healthcare, telecommunications, and logistics. The MD5 hash of this DUSTPAN sample is 17d0ada8f5610ff29f2e8eaf0e3bb578.
Strike DUSTTRAP_336a0d6f	This strike sends a malware sample known as DUSTTRAP. DUSTPAN is a multi-stage multi plugin framework with many components. First it begins by decrypting an encrypted PE file and executes this in memory. Second this decrypted PE decrypts an embedded config as well as embedded plugin dlls. Next the first plugin is observed setting up low level network communication and encryption. Finally the second plugin performs higher level network operations like downloading additional plugins to perform additional functionality. It has been associated with the Chinese state-sponsored cyber threat group APT41, and has been tied to many different sectors like healthcare, telecommunications, and logistics. The MD5 hash of this DUSTTRAP sample is 336a0d6f8cc92bf9740ce17de600463b.

<b>Name</b>	<b>Description</b>
Strike DUSTTRAP_393065ef	This strike sends a malware sample known as DUSTTRAP. DUSTPAN is a multi-stage multi plugin framework with many components. First it begins by decrypting an encrypted PE file and executes this in memory. Second this decrypted PE decrypts an embedded config as well as embedded plugin dlls. Next the first plugin is observed setting up low level network communication and encryption. Finally the second plugin performs higher level network operations like downloading additional plugins to perform additional functionality. It has been associated with the Chinese state-sponsored cyber threat group APT41, and has been tied to many different sectors like healthcare, telecommunications, and logistics. The MD5 hash of this DUSTTRAP sample is 393065ef9754e3f39b24b2d1051eab61.
Strike DUSTTRAP_8222352a	This strike sends a malware sample known as DUSTTRAP. DUSTPAN is a multi-stage multi plugin framework with many components. First it begins by decrypting an encrypted PE file and executes this in memory. Second this decrypted PE decrypts an embedded config as well as embedded plugin dlls. Next the first plugin is observed setting up low level network communication and encryption. Finally the second plugin performs higher level network operations like downloading additional plugins to perform additional functionality. It has been associated with the Chinese state-sponsored cyber threat group APT41, and has been tied to many different sectors like healthcare, telecommunications, and logistics. The MD5 hash of this DUSTTRAP sample is 8222352a61eacca3a1c6517956aa0b55.
Strike DUSTTRAP_9991ce9d	This strike sends a malware sample known as DUSTTRAP. DUSTPAN is a multi-stage multi plugin framework with many components. First it begins by decrypting an encrypted PE file and executes this in memory. Second this decrypted PE decrypts an embedded config as well as embedded plugin dlls. Next the first plugin is observed setting up low level network communication and encryption. Finally the second plugin performs higher level network operations like downloading additional plugins to perform additional functionality. It has been associated with the Chinese state-sponsored cyber threat group APT41, and has been tied to many different sectors like healthcare, telecommunications, and logistics. The MD5 hash of this DUSTTRAP sample is 9991ce9d2746313f505dbf0487337082.
Strike DUSTTRAP_a689e182	This strike sends a malware sample known as DUSTTRAP. DUSTPAN is a multi-stage multi plugin framework with many components. First it begins by decrypting an encrypted PE file and executes this in memory. Second this decrypted PE decrypts an embedded config as well as embedded plugin dlls. Next the first plugin is observed setting up low level network communication and encryption. Finally the second plugin performs higher level network operations like downloading additional plugins to perform additional functionality. It has been associated with the Chinese state-sponsored cyber threat group APT41, and has been tied to many different sectors like healthcare, telecommunications, and logistics. The MD5 hash of this DUSTTRAP sample is a689e182fe33b9d564dddc35412ea0a7.
Strike DUSTTRAP_c33247bc	This strike sends a malware sample known as DUSTTRAP. DUSTPAN is a multi-stage multi plugin framework with many components. First it begins by decrypting an encrypted PE file and executes this in memory. Second this decrypted PE decrypts an embedded config as well as embedded plugin dlls. Next the first plugin is observed setting up low level network communication and encryption. Finally the second plugin performs higher level network operations like downloading additional plugins to perform additional functionality. It has been associated with the Chinese state-sponsored cyber threat group APT41, and has been tied to many different sectors like healthcare, telecommunications, and logistics. The MD5 hash of this DUSTTRAP sample is c33247bc3e7e8cb72133e47930e6ddad.

<b>Name</b>	<b>Description</b>
Strike DUSTTRAP_cfce8554	This strike sends a malware sample known as DUSTTRAP. DUSTPAN is a multi-stage multi plugin framework with many components. First it begins by decrypting an encrypted PE file and executes this in memory. Second this decrypted PE decrypts an embedded config as well as embedded plugin dlls. Next the first plugin is observed setting up low level network communication and encryption. Finally the second plugin performs higher level network operations like downloading additional plugins to perform additional functionality. It has been associated with the Chinese state-sponsored cyber threat group APT41, and has been tied to many different sectors like healthcare, telecommunications, and logistics. The MD5 hash of this DUSTTRAP sample is cfce85548436fb89a83bf34dc17f325d.
Strike DUSTTRAP_d72f202c	This strike sends a malware sample known as DUSTTRAP. DUSTPAN is a multi-stage multi plugin framework with many components. First it begins by decrypting an encrypted PE file and executes this in memory. Second this decrypted PE decrypts an embedded config as well as embedded plugin dlls. Next the first plugin is observed setting up low level network communication and encryption. Finally the second plugin performs higher level network operations like downloading additional plugins to perform additional functionality. It has been associated with the Chinese state-sponsored cyber threat group APT41, and has been tied to many different sectors like healthcare, telecommunications, and logistics. The MD5 hash of this DUSTTRAP sample is d72f202c1d684c9a19f075290a60920f.
Strike DUSTTRAP_dc725f5e	This strike sends a malware sample known as DUSTTRAP. DUSTPAN is a multi-stage multi plugin framework with many components. First it begins by decrypting an encrypted PE file and executes this in memory. Second this decrypted PE decrypts an embedded config as well as embedded plugin dlls. Next the first plugin is observed setting up low level network communication and encryption. Finally the second plugin performs higher level network operations like downloading additional plugins to perform additional functionality. It has been associated with the Chinese state-sponsored cyber threat group APT41, and has been tied to many different sectors like healthcare, telecommunications, and logistics. The MD5 hash of this DUSTTRAP sample is dc725f5e9b1ae062fbec86ee4d816b45.
Strike DUSTTRAP_e4a4aafb	This strike sends a malware sample known as DUSTTRAP. DUSTPAN is a multi-stage multi plugin framework with many components. First it begins by decrypting an encrypted PE file and executes this in memory. Second this decrypted PE decrypts an embedded config as well as embedded plugin dlls. Next the first plugin is observed setting up low level network communication and encryption. Finally the second plugin performs higher level network operations like downloading additional plugins to perform additional functionality. It has been associated with the Chinese state-sponsored cyber threat group APT41, and has been tied to many different sectors like healthcare, telecommunications, and logistics. The MD5 hash of this DUSTTRAP sample is e4a4aafb49b8c86a5ac087ae342c0ee6.
Strike DUSTTRAP_e584119a	This strike sends a malware sample known as DUSTTRAP. DUSTPAN is a multi-stage multi plugin framework with many components. First it begins by decrypting an encrypted PE file and executes this in memory. Second this decrypted PE decrypts an embedded config as well as embedded plugin dlls. Next the first plugin is observed setting up low level network communication and encryption. Finally the second plugin performs higher level network operations like downloading additional plugins to perform additional functionality. It has been associated with the Chinese state-sponsored cyber threat group APT41, and has been tied to many different sectors like healthcare, telecommunications, and logistics. The MD5 hash of this DUSTTRAP sample is e584119a4766e6cf49093c666965c8be.

Name	Description
Strike DUSTTRAP_e98b9e21	This strike sends a malware sample known as DUSTTRAP. DUSTPAN is a multi-stage multi plugin framework with many components. First it begins by decrypting an encrypted PE file and executes this in memory. Second this decrypted PE decrypts an embedded config as well as embedded plugin dlls. Next the first plugin is observed setting up low level network communication and encryption. Finally the second plugin performs higher level network operations like downloading additional plugins to perform additional functionality. It has been associated with the Chinese state-sponsored cyber threat group APT41, and has been tied to many different sectors like healthcare, telecommunications, and logistics. The MD5 hash of this DUSTTRAP sample is e98b9e21928252332edf934f3d18ac21.
Strike DUSTTRAP_f1769ad5	This strike sends a malware sample known as DUSTTRAP. DUSTPAN is a multi-stage multi plugin framework with many components. First it begins by decrypting an encrypted PE file and executes this in memory. Second this decrypted PE decrypts an embedded config as well as embedded plugin dlls. Next the first plugin is observed setting up low level network communication and encryption. Finally the second plugin performs higher level network operations like downloading additional plugins to perform additional functionality. It has been associated with the Chinese state-sponsored cyber threat group APT41, and has been tied to many different sectors like healthcare, telecommunications, and logistics. The MD5 hash of this DUSTTRAP sample is f1769ad5a9dc44794895275c656ed484.
Strike DarkBit_9880fae6	This strike sends a malware sample known as DarkBit. The DarkBit malware is a ransomware that was recently detected in an attack targeting one of Israel's top research universities. The ransomware can accept command-line arguments or run autonomously, and it encrypts the victim's system by default with AES-256. The MD5 hash of this DarkBit sample is 9880fae6551d1e9ee921f39751a6f3c0.
Strike DarkComet_0024d4df	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 0024d4df650a7d03dae83d24097cf10.
Strike DarkComet_015d482e	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this DarkComet sample is 015d482efe46a5aa054da29a11fd9d21.
Strike DarkComet_01a2e344	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 01a2e3440d5c65442c49fe708bf94003.

<b>Name</b>	<b>Description</b>
Strike DarkComet_06844957	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 06844957c6215d0ff53804e7e5a46567.
Strike DarkComet_084b0f16	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has the timestamp field updated in the PE file header. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 084b0f165368df6f048a0aac03c55240.
Strike DarkComet_096522f8	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 096522f8c09e14d2e70723bd8d0ecd21.
Strike DarkComet_0a420405	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 0a4204058a34296805b9823fac136750.
Strike DarkComet_0ea9e3da	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has been packed using upx packer, with the default options. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 0ea9e3daf54f3bce7e88362025bfc2c1.
Strike DarkComet_117dba14	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 117dba14282c9be237e14438af11f35c.

<b>Name</b>	<b>Description</b>
Strike DarkComet_1219a18c	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 1219a18c7f3e406d8599bab3b962e2e.
Strike DarkComet_123164e8	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 123164e86411d412d6d7815f5da7a3f7.
Strike DarkComet_12ceeaa8a	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 12ceeaa8ab41fbbee00fe350ea1948eee.
Strike DarkComet_14c54f08	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 14c54f08e7b9421fc79e475494287e88.
Strike DarkComet_156fcf96	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 156fcf96d11dc0072bad9750a07a4586.
Strike DarkComet_17874dac	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has random strings (lorem ipsum) appended at the end of the file. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 17874dac85b06738e1a3bedf24c327fa.
Strike DarkComet_180f8ee1	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 180f8ee1842a3465cf9bb2e1fedce8e.

<b>Name</b>	<b>Description</b>
Strike DarkComet_19d34e15	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 19d34e15ccece451ec5c6cc8ca446a2c.
Strike DarkComet_1a7f4440	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has been packed using upx packer with the default options. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 1a7f44409dc48a420368033cc6e3c532.
Strike DarkComet_1cb232ad	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 1cb232ad0fd978eaa20c6d569d72cc64.
Strike DarkComet_1ccf967b	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 1ccf967b97a04e428c427aa7e2443e4e.
Strike DarkComet_1d84bf5f	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 1d84bf5fdfd13591e97963da8e127463.
Strike DarkComet_215b14ac	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 215b14ac07078cf72774efca6bbbfc6.
Strike DarkComet_21c6f354	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 21c6f354ae5716237ce20d781a9fe1b6.

<b>Name</b>	<b>Description</b>
Strike DarkComet_2231d047	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 2231d047078a80ee15afbee2a34d554b.
Strike DarkComet_223524c6	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 223524c6bc8859c4f43b2965a5a52aa5.
Strike DarkComet_23d09c0c	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 23d09c0cd70265deb19ccc2d87c71145.
Strike DarkComet_2448bdd7	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has been packed using upx packer, with the default options. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 2448bdd7d08f59fcf33a1de8b3f6fefd.
Strike DarkComet_24a5869b	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 24a5869bf2848684addfaa275b43b777.
Strike DarkComet_2508af1b	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 2508af1b010d477b414cca621649e4dd.
Strike DarkComet_280678a2	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 280678a2509c1a6f5f95251ae64f8ea9.

<b>Name</b>	<b>Description</b>
Strike DarkComet_3020a3cf	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 3020a3cf445d52f1e270be0f61154dce.
Strike DarkComet_31cc19f2	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 31cc19f2cc08e7df9711899b6c27fd92.
Strike DarkComet_32ed49d7	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 32ed49d7aacbf433448690794ffa9cd0.
Strike DarkComet_3384f056	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 3384f05676215c2d78e9c66a11ee47a0.
Strike DarkComet_356cc373	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has random contents appended in one of the existing sections in the PE file format. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 356cc3735d57b3a84584561c260dfc66.
Strike DarkComet_37ca3c3b	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The binary has the checksum removed in the PE file format. The MD5 hash of this DarkComet sample is 37ca3c3b0beed927bb5e6f8954975364.

<b>Name</b>	<b>Description</b>
Strike DarkComet_38353d77	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 38353d77489a0a4c074fa0754481b847.
Strike DarkComet_3e0bc2a9	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 3e0bc2a9652485354c3eeae5cd098261.
Strike DarkComet_3e6c1c04	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system.The binary has the timestamp field updated in the PE file header. The MD5 hash of this DarkComet sample is 3e6c1c04f9810c8d0ae4a55753a5f304.
Strike DarkComet_415042b1	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system.The binary has been packed using upx packer, with the default options. The MD5 hash of this DarkComet sample is 415042b1569d57425f241de1375e95ad.
Strike DarkComet_43e6cebc	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 43e6cebc5006c35d2566de39f4e008cf.
Strike DarkComet_46c9ea27	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 46c9ea27274f4a7685f801c47c08e5df.

<b>Name</b>	<b>Description</b>
Strike DarkComet_4728b416	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 4728b41696a634edc12be912acf8cd82.
Strike DarkComet_4a7e069e	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 4a7e069efb5972d4d99a9161b6b36f40.
Strike DarkComet_506f3057	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 506f3057b3a4ea70644ec59d6d591b81.
Strike DarkComet_520560d0	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 520560d0a4f433a735ddc5c316fbcd24.
Strike DarkComet_520f4745	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 520f4745b30071068ed610873843c165.
Strike DarkComet_525c90b0	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has random strings (lorem ipsum) appended at the end of the file. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 525c90b09a41da79d49ba246b6c2e5c1.
Strike DarkComet_5288ee62	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 5288ee620e47eff39ba4db70e62e249b.

<b>Name</b>	<b>Description</b>
Strike DarkComet_52a36eb8	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 52a36eb898a816a12e52f81c2160adb3.
Strike DarkComet_52dc384a	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system.The binary has random bytes appended at the end of the file. The MD5 hash of this DarkComet sample is 52dc384a398e644786a67e03ce9011c7.
Strike DarkComet_55f9fbdf	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system.The binary has random strings (lorem ipsum) appended at the end of the file. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 55f9fbdfbec0c1160c66e97c6e9b93e8.
Strike DarkComet_5bd6a495	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system.The binary has random bytes appended at the end of the file. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 5bd6a4959e85dc87e9fcd0da98bd36ab.
Strike DarkComet_5de32a2e	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 5de32a2ef97290585b28f4409384251a.
Strike DarkComet_5fdfd1ed	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system.The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this DarkComet sample is 5fdfd1edd86e6752cc76e9de5d5d17e1.

<b>Name</b>	<b>Description</b>
Strike DarkComet_5ff45a27	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this DarkComet sample is 5ff45a27e2c9d3708240303a78e0be6e.
Strike DarkComet_6246b3fa	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 6246b3fab642506182bd3cfe2b08f071.
Strike DarkComet_638854bf	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 638854bf5d54769e559abdd901b40579.
Strike DarkComet_646128de	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has a random section name renamed according to the PE format specification. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 646128de2317254aec6537a834acc16e.
Strike DarkComet_653637f3	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has the timestamp field updated in the PE file header. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 653637f3f83f6d22682cca41ff86c6d5.
Strike DarkComet_65a19a73	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is 65a19a730f50c5daea17f95adf114c90.

<b>Name</b>	<b>Description</b>
Strike DarkComet_69f9e1ec	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has random strings (lorem ipsum) appended at the end of the file. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 69f9e1ec5caa6b033f9a7f4eb65c3d52.
Strike DarkComet_6b41728e	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has been packed using upx packer, with the default options. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 6b41728e3ab0def43977ee60ea6efa.
Strike DarkComet_6d0ab127	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 6d0ab12741204e06e5b8ddcf1ebd4e76.
Strike DarkComet_6d8497e4	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 6d8497e484b8c215c417bea6db3b5550.
Strike DarkComet_6f2fdbda	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 6f2fdbdadd5bc65bcda1a5450aafc7a3.
Strike DarkComet_71be9b56	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 71be9b56b5d518b855fefbd3514bbc09.

<b>Name</b>	<b>Description</b>
Strike DarkComet_74fa1e21	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has random strings (lorem ipsum) appended at the end of the file. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 74fa1e218c757e3745df3add55fff2c6.
Strike DarkComet_751f9f9d	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 751f9f9de9d38623fe0c1fd867e7782f.
Strike DarkComet_76771df5	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has the timestamp field updated in the PE file header. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 76771df5c70cdcfb31d6ac6d2eb0fe9c.
Strike DarkComet_7a1a393e	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 7a1a393eb5215996cabd8346bcb7eb10.
Strike DarkComet_7a7a2615	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 7a7a261530db35879c9c080cc46084de.
Strike DarkComet_7ada5970	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 7ada5970aa4eaeff202d0e67d872ee2e.

<b>Name</b>	<b>Description</b>
Strike DarkComet_82c13f1a	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 82c13f1ae5f54f140e91b1f06187fc4c.
Strike DarkComet_82ca4f6e	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 82ca4f6e2a35aa52ff49aa5c61a905b5.
Strike DarkComet_83530a3b	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 83530a3bb89f17a0fd991f7813c97cd3.
Strike DarkComet_853a59fd	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 853a59fdea0237da61f6bd8119eaedfe.
Strike DarkComet_8f371632	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has the timestamp field updated in the PE file header. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 8f3716323dee1adc19440a1a0ea4cbb7.
Strike DarkComet_9798305f	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 9798305f8ecb993465ae08c4fefc4688.
Strike DarkComet_97eebf03	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 97eebf03ca937627e7a35c84503ceb2d.

<b>Name</b>	<b>Description</b>
Strike DarkComet_99ddecdd	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 99ddecdd7bf0b3c8ee071b8876c77b0e.
Strike DarkComet_9c8da8ae	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has been packed using upx packer with the default options. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 9c8da8ae53f23da497a103cb532e06ab.
Strike DarkComet_9ddc588c	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is 9ddc588c0382050b2a736c2a2ad6ccb0.
Strike DarkComet_a6eafe7f	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is a6eafe7f3fa6053ef50baa7c167ace49.
Strike DarkComet_a8ad7b28	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has random bytes appended at the end of the file. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is a8ad7b28b6b312633f97d542d3e18c66.
Strike DarkComet_aaf9800c	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is aaf9800c6ebda965c676c580dee47186.

<b>Name</b>	<b>Description</b>
Strike DarkComet_ac34dce8	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is ac34dce8050f844dd3927018a2e365f1.
Strike DarkComet_ad8417d8	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has the timestamp field updated in the PE file header. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is ad8417d8eaacf3b633b9bead2ee3ef87.
Strike DarkComet_af7e1cf	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is af7e1cf7d0c1dcf3e55e57590286549.
Strike DarkComet_b06f43f7	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is b06f43f7f11d71d39ee45e745767928f.
Strike DarkComet_b2a17564	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is b2a17564d97ec1ca975dc8ee222a987.
Strike DarkComet_b462b913	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is b462b9138b52341cd8db3aff6f7afee6.
Strike DarkComet_b55b6a3c	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is b55b6a3cda5fc405305550d50b5fa817.

<b>Name</b>	<b>Description</b>
Strike DarkComet_b6e67772	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has random bytes appended at the end of the file. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is b6e677725ccab82655970e14e88c61d8.
Strike DarkComet_b84ab2c0	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is b84ab2c079ef2e9dad478abc81e3dee0.
Strike DarkComet_b88fa8ad	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is b88fa8add9ac38d0507751f35edfc183.
Strike DarkComet_b8a44c83	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has random bytes appended at the end of the file. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is b8a44c83650a1416fa661c9ed44529ea.
Strike DarkComet_be43f6c3	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is be43f6c3f4445ab4aa4d75cb1f2b1e9d.
Strike DarkComet_c2245f15	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is c2245f152402595fa0591418cf55d290.

<b>Name</b>	<b>Description</b>
Strike DarkComet_c288a312	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has random contents appended in one of the existing sections in the PE file format. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is c288a31269c6d2b85e08603cf6eafe4.
Strike DarkComet_c2f62b1b	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is c2f62b1bcfae0de0c672cbe79e56064c.
Strike DarkComet_c35d5775	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is c35d5775dd66aab590f8e41ca16c1b4a.
Strike DarkComet_c42a46b5	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is c42a46b589226ebe80a14412b6fef211.
Strike DarkComet_c86fdaf2	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has been packed using upx packer, with the default options. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is c86fdaf22f4d47641972808993f183b9.
Strike DarkComet_c8e7b11f	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is c8e7b11fa51f2ae03e9cb863b55df78d.

<b>Name</b>	<b>Description</b>
Strike DarkComet_cb2776d1	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has a random section name renamed according to the PE format specification. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is cb2776d128575116707d78e3bd858fb2.
Strike DarkComet_cf9031f5	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The binary has the debug flag removed in the PE file format. The MD5 hash of this DarkComet sample is cf9031f5f60e4c6dc23faa0a3a1d5b9b.
Strike DarkComet_d619583b	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is d619583b03bae980edca49feede8579c.
Strike DarkComet_d6b4318e	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is d6b4318e91f5422c2a55a9b40228a365.
Strike DarkComet_dacded52	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is dacded526944ecb98ddd58f543141c84.
Strike DarkComet_dbf7ba48	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has a random section name renamed according to the PE format specification. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system. The MD5 hash of this DarkComet sample is dbf7ba480e7019322a3c7b12bcee3060.

<b>Name</b>	<b>Description</b>
Strike DarkComet_dd9c342a	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has a random section name renamed according to the PE format specification. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is dd9c342a0c4ce50441af2794586eb243.
Strike DarkComet_df4a6de4	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is df4a6de44c1341c71251aa7b1930cf6f.
Strike DarkComet_e0ba1170	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is e0ba1170722739bd05a56e350eb08310.
Strike DarkComet_e34111d9	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is e34111d9e2ddbea03a6cd91236f4dc27.
Strike DarkComet_e439db25	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is e439db25dd10f03b22cedc55b1e47b90.
Strike DarkComet_e5df0db4	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is e5df0db41a655829f3564fb6d45f527a.
Strike DarkComet_e9398ac5	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is e9398ac53c135781e952477e91fb02c.

<b>Name</b>	<b>Description</b>
Strike DarkComet_ea184546	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has a random section name renamed according to the PE format specification. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is ea1845464d317ae08f1f994797df1340.
Strike DarkComet_eab4cfa5	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is eab4cfa5c8a4af29ee1727f9814dc806.
Strike DarkComet_eb1de375	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is eb1de375f155cf314cd6f41f754ce930.
Strike DarkComet_eceac426	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is eceac426ece31db82c011c3925d1561a.
Strike DarkComet_eda137e5	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is eda137e5ecbae3a6e14adc9266ccf038.
Strike DarkComet_ef078a83	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is ef078a8364715c9e2c9ec6441db3aa0b.
Strike DarkComet_f09ebc3e	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is f09ebc3e8c61f3cc45059c41857f36fb.

<b>Name</b>	<b>Description</b>
Strike DarkComet_f1672da4	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has the checksum removed in the PE file format. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is f1672da40e317021e8e81a73de0aeaa3.
Strike DarkComet_f5491800	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is f5491800859ca7512dc4839225543a2d.
Strike DarkComet_f8fa861a	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is f8fa861a87d39fb63a9b0dff18a24d90.
Strike DarkComet_fac38e7a	This strike sends a polymorphic malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. The binary has random bytes appended at the end of the file. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is fac38e7afa79375ca964db486879bfef.
Strike DarkComet_fdb454b6	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is fdb454b644e210f2b986295d8d25d383.
Strike DarkComet_ffc9ea7f	This strike sends a malware sample known as DarkComet. DarkComet and related variants are a family of remote access trojans designed to provide an attacker with control over an infected system. Capabilities of this malware include the ability to download files from a user's machine, mechanisms for persistence and hiding, and the ability to send back usernames and passwords from the infected system The MD5 hash of this DarkComet sample is ffc9ea7f613f903d31218a0b3394600a.
Strike DarkKomet_07cd9307	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 07cd93078bf5a5a28360fce833ac75a3.

<b>Name</b>	<b>Description</b>
Strike DarkKomet_0e5bc969	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 0e5bc9695442dcabb77be26c203708e3.
Strike DarkKomet_16b1b477	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 16b1b477b093a551a88d1e62a340cd94.
Strike DarkKomet_1c4705bc	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 1c4705bccd3a8c4992eeab0daeb63a49.
Strike DarkKomet_296477f4	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 296477f4a6ee0696f492ab955578f1a2.
Strike DarkKomet_29749cd4	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 29749cd4791f34d76d620d80b833f307.
Strike DarkKomet_31f421d6	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 31f421d6f9684d27cbf27bf9f50049ee.
Strike DarkKomet_472cf260	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 472cf260266980cbbed9d6054ee1d161.
Strike DarkKomet_52db481d	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 52db481d13883721bdeec442a293781.

<b>Name</b>	<b>Description</b>
Strike DarkKomet_535f56be	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 535f56be2c6bd965548864e65e1433c6.
Strike DarkKomet_602d5277	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 602d5277edc95076d58c33dd2dde428e.
Strike DarkKomet_64916b96	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 64916b96176449c7aec4d0adec055111.
Strike DarkKomet_6c7bb741	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 6c7bb74133fa4462f030de13415108d1.
Strike DarkKomet_758f1590	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 758f159012adf559276f74dec143e4f1.
Strike DarkKomet_88123242	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 88123242d631fb205b49827cabb3a306.
Strike DarkKomet_8ecfcfd69	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 8ecfcfd699de69ff65a3cd3f6b6de329b.
Strike DarkKomet_95b89858	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 95b8985804bcb843b80594617f027c52.

<b>Name</b>	<b>Description</b>
Strike DarkKomet_9d801556	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 9d801556b05b156c65a6fcc06157ec47.
Strike DarkKomet_9ff86eff	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is 9ff86eff19a08360ed26733e73e71abd.
Strike DarkKomet_c311aa40	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is c311aa4054689cce23a9d3daa0188312.
Strike DarkKomet_c633939e	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is c633939e77b5cad28435cd6d1992f733.
Strike DarkKomet_d67857bf	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is d67857bf55235d7bd2af03785e61073f.
Strike DarkKomet_eb6eda8d	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is eb6eda8d9e47e427383fb7a2c33e0591.
Strike DarkKomet_fca9ed0f	This strike sends a malware sample known as DarkKomet. DarkKomet is a freeware remote access trojan that was released by an independent software developer. It provides the same functionality you would expect from a remote access tool: keylogging, webcam access, microphone access, remote desktop, URL download, program execution, etc. The MD5 hash of this DarkKomet sample is fca9ed0f8759e5c71e0911cd6e819273.

<b>Name</b>	<b>Description</b>
Strike DarkSide_01cef4d4	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 01cef4d4f9306177d42f221854ee552b.
Strike DarkSide_0240d59b	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 0240d59b0275e347fb5c3916cc8720e6.
Strike DarkSide_0390938e	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 0390938e8a9df14af45e264a128a5bf8.
Strike DarkSide_04fde434	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 04fde4340cc79cd9e61340d4c1e8ddfb.
Strike DarkSide_0e178c48	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 0e178c4808213ce50c2540468ce409d3.
Strike DarkSide_0ed51a59	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 0ed51a595631e9b4d60896ab557332f.
Strike DarkSide_130220f4	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 130220f4457b9795094a21482d5f104b.

<b>Name</b>	<b>Description</b>
Strike DarkSide_1a57e37d	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 1a57e37d4160446c7b5ec4991fd049a1.
Strike DarkSide_1a700f84	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 1a700f845849e573ab3148daef1a3b0b.
Strike DarkSide_1c33dc87	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 1c33dc87c6fdb80725d732a5323341f9.
Strike DarkSide_2201ca26	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 2201ca264fed0d997da6c5701af7e591.
Strike DarkSide_222792d2	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 222792d2e75782516d653d5ccfcf33b.
Strike DarkSide_25b60dd7	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 25b60dd786811e7453cedef90558fba6.
Strike DarkSide_29bcd459	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 29bcd459f5ddeefad26fc098304e786.

<b>Name</b>	<b>Description</b>
Strike DarkSide_2c79d66f	This strike sends a polymorphic malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this DarkSide sample is 2c79d66f1dc05a065ad409813c60feeb.
Strike DarkSide_2f31ce15	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 2f31ce153a8f1d9e30e8ee7305ee7a6a.
Strike DarkSide_31ecfd98	This strike sends a polymorphic malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this DarkSide sample is 31ecfd9898a51b1b116d6805a7ed06b5.
Strike DarkSide_39db5648	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 39db5648c2ddef913989f51c711b1356.
Strike DarkSide_3fd9b011	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 3fd9b0117a0e79191859630148dc6d.
Strike DarkSide_47a4420a	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 47a4420ad26f60bb6bba5645326fa963.

<b>Name</b>	<b>Description</b>
Strike DarkSide_4d3471d8	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 4d3471d8513626e992936e4065b2d87d.
Strike DarkSide_4d419dc5	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 4d419dc50e3e4824c096f298e0fa885a.
Strike DarkSide_4ed7cd93	This strike sends a polymorphic malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The binary has been packed using upx packer, with the default options. The MD5 hash of this DarkSide sample is 4ed7cd9394bba49ed36c657d2a7ca0a6.
Strike DarkSide_5d5a210c	This strike sends a polymorphic malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this DarkSide sample is 5d5a210c1f095c039a5c2cb2411391ac.
Strike DarkSide_5ff75d33	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 5ff75d33080bb97a8e6b54875c221777.
Strike DarkSide_66ddb290	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 66ddb290df3d510a6001365c3a694de2.

<b>Name</b>	<b>Description</b>
Strike DarkSide_68ada5f6	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 68ada5f6aa8e3c3969061e905ceb204c.
Strike DarkSide_69ec3d13	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 69ec3d1368adbe75f3766fc88bc64afc.
Strike DarkSide_6a7fdab1	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 6a7fdab1c7f6c5a5482749be5c4bf1a4.
Strike DarkSide_6e6278fa	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 6e6278fa8eda2c2b2ce8fac2ba78cdcc.
Strike DarkSide_72a14a67	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 72a14a67df04b4c3b7423a4120082785.
Strike DarkSide_84c15679	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 84c1567969b86089cc33dccf41562bcd.
Strike DarkSide_885fc8fb	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 885fc8fb590b899c1db7b42fe83dddc3.

<b>Name</b>	<b>Description</b>
Strike DarkSide_88c02d90	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 88c02d9088cdd0bff565b294be887c69.
Strike DarkSide_904805c6	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 904805c6f368acaf024c1fe09279230c.
Strike DarkSide_91e28079	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 91e2807955c5004f13006ff795cb803c.
Strike DarkSide_979692cd	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 979692cd7fc638beea6e9d68c752f360.
Strike DarkSide_9d418ecc	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 9d418ecc0f3bf45029263b0944236884.
Strike DarkSide_9e779da8	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is 9e779da82d86bcd4cc43ab29f929f73f.
Strike DarkSide_a3d964aa	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is a3d964aaf642d626474f02ba3ae4f49b.

<b>Name</b>	<b>Description</b>
Strike DarkSide_a8690b73	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is a8690b739971d63318ad4895b9c41058.
Strike DarkSide_ac4b1759	This strike sends a polymorphic malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The binary has the checksum removed in the PE file format. The MD5 hash of this DarkSide sample is ac4b1759f73f6abc497decdbc53011cb.
Strike DarkSide_b0fd4516	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is b0fd45162c2219e14bdccab76f33946e.
Strike DarkSide_b2011e98	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is b2011e987b85a8005d9bd3a33ff6e1b6.
Strike DarkSide_b278d7ec	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is b278d7ec3681df16a541cf9e34d3b70a.
Strike DarkSide_b3a6f3f4	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is b3a6f3f471728db2be40a2ff77b18fa4.
Strike DarkSide_b68be0da	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is b68be0dacf09904cd4a0fbe0aab3842e.

<b>Name</b>	<b>Description</b>
Strike DarkSide_b9d04060	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is b9d04060842f71d1a8f3444316dc1843.
Strike DarkSide_c2764be5	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is c2764be55336f83a59aa0f63a0b36732.
Strike DarkSide_c2fb8ddb	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is c2fb8ddbbf2fc8527b5d7a5a2015e26a.
Strike DarkSide_c363e327	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is c363e327287081251b820276cd9ce1f8.
Strike DarkSide_c4f1a1b7	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is c4f1a1b73e4af0fbb63af8ee89a5a7fe.
Strike DarkSide_c81dae5c	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is c81dae5c67fb72a2c2f24b178aea50b7.
Strike DarkSide_c8305125	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is c830512579b0e08f40bc1791fc10c582.

<b>Name</b>	<b>Description</b>
Strike DarkSide_ce7b2f70	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is ce7b2f7008ab93c659494f2931160147.
Strike DarkSide_cee2fc1d	This strike sends a polymorphic malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The binary file has one more imports added in the import table. The MD5 hash of this DarkSide sample is cee2fc1d45b94d4c4ff5acbcd664212.
Strike DarkSide_ceed9cee	This strike sends a polymorphic malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The binary has random bytes appended at the end of the file. The MD5 hash of this DarkSide sample is ceed9cee94852c38da142b4686c11560.
Strike DarkSide_cfcfb689	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is cfcfb68901ffe513e9f0d76b17d02f96.
Strike DarkSide_d6634959	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is d6634959e4f9b42dfc02b270324fa6d9.
Strike DarkSide_dec3eb5c	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is dec3eb5c3db86ecbad95d50fea19adc1.

<b>Name</b>	<b>Description</b>
Strike DarkSide_e409ad05	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is e409ad05784d25f2714274db52fde8b7.
Strike DarkSide_e4445015	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is e44450150e8683a0addd5c686cd4d202.
Strike DarkSide_e5ca2d12	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is e5ca2d127e7300f28fbef1e74d6a6858.
Strike DarkSide_e705dfb2	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is e705dfb2d66af2c64f03730f670f1d54.
Strike DarkSide_edb56705	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is edb5670581d49771d180940c4d1179b1.
Strike DarkSide_f00aded4	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is f00aded4c16c0e8c3b5adfc23d19c609.
Strike DarkSide_f587adbd	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines in 2021 when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is f587adbd83ff3f4d2985453cd45c7ab1.

<b>Name</b>	<b>Description</b>
Strike DarkSide_f75ba194	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is f75ba194742c978239da2892061ba1b4.
Strike DarkSide_f87a2e1c	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware that made headlines recently when it was attributed to the attack against CompuCom resulting in 20 million dollars in losses. DarkSide is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is f87a2e1c3d148a67eaeb696b1ab69133.
Strike DarkSide_f913d43b	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is f913d43ba0a9f921b1376b26cd30fa34.
Strike DarkSide_f9fc1a1a	This strike sends a malware sample known as DarkSide. DarkSide is a ransomware group that made headlines recently when it was attributed to the attack against CompuCom as well as an attack against the Colonial Pipeline, taking the major US fuel pipeline offline. The DarkSide group is known for its very specific approach to targeting victims. Each executable is carefully crafted for its intended target. The MD5 hash of this DarkSide sample is f9fc1a1a95d5723c140c2a8effc93722.
Strike DarkTortilla Loader_6312c27d	This strike sends a polymorphic malware sample known as DarkTortilla Loader. DarkTortilla is a .NET-based crypter that delivers information stealers and remote access trojans like AgentTesla and RedLine. It has also been observed delivering payloads like Cobalt Strike and Metasploit as well as other malicious documents and executables. This sample is the DarkTortilla initial loader. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this DarkTortilla Loader sample is 6312c27d72dfca46e9dc99030ce5e944.
Strike DarkTortilla Loader_6e91ad09	This strike sends a malware sample known as DarkTortilla Loader. DarkTortilla is a .NET-based crypter that delivers information stealers and remote access trojans like AgentTesla and RedLine. It has also been observed delivering payloads like Cobalt Strike and Metasploit as well as other malicious documents and executables. This sample is the DarkTortilla initial loader. The MD5 hash of this DarkTortilla Loader sample is 6e91ad0972e104a277505104abe39d1e.
Strike DarkTortilla Loader_76d32fe3	This strike sends a polymorphic malware sample known as DarkTortilla Loader. DarkTortilla is a .NET-based crypter that delivers information stealers and remote access trojans like AgentTesla and RedLine. It has also been observed delivering payloads like Cobalt Strike and Metasploit as well as other malicious documents and executables. This sample is the DarkTortilla initial loader. The binary has the timestamp field updated in the PE file header. The MD5 hash of this DarkTortilla Loader sample is 76d32fe38d0b95c1736133b944b08e56.

<b>Name</b>	<b>Description</b>
Strike DarkTortilla Loader_7b31ea74	This strike sends a polymorphic malware sample known as DarkTortilla Loader. DarkTortilla is a .NET-based crypter that delivers information stealers and remote access trojans like AgentTesla and RedLine. It has also been observed delivering payloads like Cobalt Strike and Metasploit as well as other malicious documents and executables. This sample is the DarkTortilla initial loader. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this DarkTortilla Loader sample is 7b31ea74f3666a5c53683df6b6c98539.
Strike DarkTortilla Loader_827258f9	This strike sends a malware sample known as DarkTortilla Loader. DarkTortilla is a .NET-based crypter that delivers information stealers and remote access trojans like AgentTesla and RedLine. It has also been observed delivering payloads like Cobalt Strike and Metasploit as well as other malicious documents and executables. This sample is the DarkTortilla initial loader. The MD5 hash of this DarkTortilla Loader sample is 827258f907c5087f498c413d28e2203e.
Strike DarkTortilla Loader_84872b60	This strike sends a malware sample known as DarkTortilla Loader. DarkTortilla is a .NET-based crypter that delivers information stealers and remote access trojans like AgentTesla and RedLine. It has also been observed delivering payloads like Cobalt Strike and Metasploit as well as other malicious documents and executables. This sample is the DarkTortilla initial loader. The MD5 hash of this DarkTortilla Loader sample is 84872b60072011eab8940f3b49bdb582.
Strike DarkTortilla Loader_851816aa	This strike sends a malware sample known as DarkTortilla Loader. DarkTortilla is a .NET-based crypter that delivers information stealers and remote access trojans like AgentTesla and RedLine. It has also been observed delivering payloads like Cobalt Strike and Metasploit as well as other malicious documents and executables. This sample is the DarkTortilla initial loader. The MD5 hash of this DarkTortilla Loader sample is 851816aa8cf45ba769f0d9420acfb3e5.
Strike DarkTortilla Loader_8d8c551d	This strike sends a malware sample known as DarkTortilla Loader. DarkTortilla is a .NET-based crypter that delivers information stealers and remote access trojans like AgentTesla and RedLine. It has also been observed delivering payloads like Cobalt Strike and Metasploit as well as other malicious documents and executables. This sample is the DarkTortilla initial loader. The MD5 hash of this DarkTortilla Loader sample is 8d8c551dd572a1dc158de239b37eaa9a.
Strike DarkTortilla Loader_93fe6600	This strike sends a malware sample known as DarkTortilla Loader. DarkTortilla is a .NET-based crypter that delivers information stealers and remote access trojans like AgentTesla and RedLine. It has also been observed delivering payloads like Cobalt Strike and Metasploit as well as other malicious documents and executables. This sample is the DarkTortilla initial loader. The MD5 hash of this DarkTortilla Loader sample is 93fe6600c51014d7d6c2afedf8398f92.
Strike DarkTortilla Loader_c37aae0f	This strike sends a malware sample known as DarkTortilla Loader. DarkTortilla is a .NET-based crypter that delivers information stealers and remote access trojans like AgentTesla and RedLine. It has also been observed delivering payloads like Cobalt Strike and Metasploit as well as other malicious documents and executables. This sample is the DarkTortilla initial loader. The MD5 hash of this DarkTortilla Loader sample is c37aae0ff565a2e44f144f837b750279.

<b>Name</b>	<b>Description</b>
Strike DarkTortilla Loader_cd49f7c3	This strike sends a malware sample known as DarkTortilla Loader. DarkTortilla is a .NET-based crypter that delivers information stealers and remote access trojans like AgentTesla and RedLine. It has also been observed delivering payloads like Cobalt Strike and Metasploit as well as other malicious documents and executables. This sample is the DarkTortilla initial loader. The MD5 hash of this DarkTortilla Loader sample is cd49f7c3c4e82dee128eedea9879bc33.
Strike DarkTortilla Loader_f44695a8	This strike sends a malware sample known as DarkTortilla Loader. DarkTortilla is a .NET-based crypter that delivers information stealers and remote access trojans like AgentTesla and RedLine. It has also been observed delivering payloads like Cobalt Strike and Metasploit as well as other malicious documents and executables. This sample is the DarkTortilla initial loader. The MD5 hash of this DarkTortilla Loader sample is f44695a8febb2a35576a59fa984629d2.
Strike Darkgate DLL_9d82885d	This strike sends a malware sample known as Darkgate DLL. This sample is a DLL associated with Darkgate. Darkgate is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. The malware employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate DLL sample is 9d82885d1f60a13f2a8d16288739684c.
Strike Darkgate Loader_645cc995	This strike sends a malware sample known as Darkgate Loader. This sample is a loader associated with Darkgate. The shellcode loader downloads, decrypts, and executes the final payload. Darkgate is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. The malware employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate Loader sample is 645cc995139d0646250eca32683afae1.

Name	Description
Strike Darkgate Loader_b4aa788e	<p>This strike sends a malware sample known as Darkgate Loader. This sample is a loader associated with Darkgate. The shellcode loader downloads, decrypts, and executes the final payload. Darkgate is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. The malware employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate Loader sample is b4aa788e1ca35302f67d344b82e6ed47.</p>
Strike Darkgate Shellcode_9ef277f5	<p>This strike sends a malware sample known as Darkgate Shellcode. This sample is a shellcode associated with Darkgate. The shellcode is responsible for executing a PE file that acts as the DarkGate loader module. Darkgate is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. The malware employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate Shellcode sample is 9ef277f5ff3ad7137e03ad3f10ca60a2.</p>
Strike Darkgate VBS_5f654c88	<p>This strike sends a malware sample known as Darkgate VBS. This sample is a VBS script associated with Darkgate. The initial VBS dropper contains obfuscated code when executed it downloads and executes a Windows batch script from the command and control (C2) server. Darkgate is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. The malware employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate VBS sample is 5f654c882635686b095afb36fd03060d.</p>

Name	Description
Strike Darkgate VBS_726bda47	<p>This strike sends a malware sample known as Darkgate VBS. This sample is a VBS script associated with Darkgate. The initial VBS dropper contains obfuscated code when executed it downloads and executes a Windows batch script from the command and control (C2) server. Darkgate is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. The malware employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate VBS sample is 726bda475bacd81fb0887a313635f3aa.</p>
Strike Darkgate_1b9e9d90	<p>This strike sends a malware sample known as Darkgate. This sample belongs to DarkGate. It is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. DarkGate employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate sample is 1b9e9d90136d033a52d2c282503f33b7.</p>
Strike Darkgate_2989dab1	<p>This strike sends a malware sample known as Darkgate. This sample belongs to DarkGate. It is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. DarkGate employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate sample is 2989dab1e3196f06c6ac6abb8693f27d.</p>
Strike Darkgate_63f9b76e	<p>This strike sends a malware sample known as Darkgate. This sample belongs to DarkGate. It is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. DarkGate employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate sample is 63f9b76e4bf4983e13eba7e22dd22781.</p>

<b>Name</b>	<b>Description</b>
Strike Darkgate_82c7c522	<p>This strike sends a malware sample known as Darkgate. This sample belongs to DarkGate. It is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. DarkGate employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate sample is 82c7c522cdc0901d92b51e3134694ce0.</p>
Strike Darkgate_83037a44	<p>This strike sends a malware sample known as Darkgate. This sample belongs to DarkGate. It is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. DarkGate employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate sample is 83037a444567a6d47b6221288cdad4e9.</p>
Strike Darkgate_9bf2ae2d	<p>This strike sends a malware sample known as Darkgate. This sample belongs to DarkGate. It is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. DarkGate employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate sample is 9bf2ae2da16e9a975146c213abd7cd4f.</p>
Strike Darkgate_bce3f0e9	<p>This strike sends a malware sample known as Darkgate. This sample belongs to DarkGate. It is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. DarkGate employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate sample is bce3f0e952e0f9a39b725fb38192b940.</p>

Name	Description
Strike Darkgate_df2606b1	This strike sends a malware sample known as Darkgate. This sample belongs to DarkGate. It is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. DarkGate employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate sample is df2606b108c4f28049f37d91b41150a5.
Strike Darkgate_f242ce46	This strike sends a malware sample known as Darkgate. This sample belongs to DarkGate. It is a Remote Access Trojan (RAT) offered as Malware-as-a-Service (MaaS) which poses a formidable threat designed to achieve full system compromise. DarkGate employs extensive evasion tactics, command and control features, and modules for credential theft, keylogging, and screen capturing. It's widely adopted by cybercriminals globally. Delivery channels include phishing emails with links to Visual Basic Script (VBS) or Microsoft Software Installer (MSI) files. Recent tactics involve using collaborative apps like Microsoft Teams. The malware is delivered via a deceptive ZIP file containing Windows shortcut files, executing a Windows Batch script to retrieve, and run a remote VBS script. The MD5 hash of this Darkgate sample is f242ce468771de8c7a23568a3b03a5e2.
Strike Deadbolt_1b5d415e	This strike sends a malware sample known as Deadbolt. Deadbolt malware is a ransomware that was first seen targeting QNAP NAS devices during Jan 2022. It has a multi-tiered payment and extortion scheme, a flexible configuration, and is heavily automated. The MD5 hash of this Deadbolt sample is 1b5d415eeb8d926fc当地caec6e345c5d0c1。
Strike Deadbolt_5e185a8b	This strike sends a malware sample known as Deadbolt. Deadbolt malware is a ransomware that was first seen targeting QNAP NAS devices during Jan 2022. It has a multi-tiered payment and extortion scheme, a flexible configuration, and is heavily automated. The MD5 hash of this Deadbolt sample is 5e185a8b4077a9149fa5cc6ae2bea12c.
Strike Deadbolt_6821f568	This strike sends a malware sample known as Deadbolt. Deadbolt malware is a ransomware that was first seen targeting QNAP NAS devices during Jan 2022. It has a multi-tiered payment and extortion scheme, a flexible configuration, and is heavily automated. The MD5 hash of this Deadbolt sample is 6821f568af50383f31ceac886a99ab7.
Strike Deadbolt_718ae697	This strike sends a malware sample known as Deadbolt. Deadbolt malware is a ransomware that was first seen targeting QNAP NAS devices during Jan 2022. It has a multi-tiered payment and extortion scheme, a flexible configuration, and is heavily automated. The MD5 hash of this Deadbolt sample is 718ae69788dc752a8db46b0e43e42f13.

<b>Name</b>	<b>Description</b>
Strike Deadbolt_76022a94	This strike sends a malware sample known as Deadbolt. Deadbolt malware is a ransomware that was first seen targeting QNAP NAS devices during Jan 2022. It has a multi-tiered payment and extortion scheme, a flexible configuration, and is heavily automated. The MD5 hash of this Deadbolt sample is 76022a94288bbb07e22d8509b37eea71.
Strike Deadbolt_f2bf3c75	This strike sends a malware sample known as Deadbolt. Deadbolt malware is a ransomware that was first seen targeting QNAP NAS devices during Jan 2022. It has a multi-tiered payment and extortion scheme, a flexible configuration, and is heavily automated. The MD5 hash of this Deadbolt sample is f2bf3c75b172112d492d985917064f0b.
Strike DeceptiveDevelopment_250 443d3	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is 250443d3d3fe43e9d0ecacba69130842.
Strike DeceptiveDevelopment_3ae d5502	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is 3aed5502118eb9b8c9f8a779d4b09e11.
Strike DeceptiveDevelopment_3ef7 717c	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is 3ef7717c8bcb26396fc50ed92e812d13.
Strike DeceptiveDevelopment_535 03cbe	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is 53503cbe1d3f62e4b5fd3245ce144858.

<b>Name</b>	<b>Description</b>
Strike DeceptiveDevelopment_617 5efd1	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is 6175efd148a89ca61b6835c77acc7a8d.
Strike DeceptiveDevelopment_6d7 68860	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is 6d76886042d1d6957fec9b60cb4cc78d.
Strike DeceptiveDevelopment_a00 9cd35	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is a009cd35850929199ef60e71bce86830.
Strike DeceptiveDevelopment_b29 ddcc9	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is b29ddcc9affdd56a520f23a61b670134.
Strike DeceptiveDevelopment_b52 e105b	This strike sends a malware sample known as DeceptiveDevelopment. DeceptiveDevelopment is a malware that evolves from primitive crypto theft to sophisticated AI-based deception. It is typically delivered via phishing emails containing malicious attachments. Upon execution, the malware deploys a series of scripts to steal sensitive information, and later versions even utilize AI to mimic human behavior and deceive security systems. Its key capabilities involve stealing cryptocurrency wallet information, exfiltrating user data, and mimicking human behavior to evade detection. The MD5 hash of this DeceptiveDevelopment sample is b52e105bd040bda6639e958f7d9e3090.

<b>Name</b>	<b>Description</b>
Strike Defray777_210f47c8	This strike sends a malware sample known as Defray777. Defray777 is an elusive family of Ransomware also known as RansomX and RansomExx that has been active since 2018. It runs entirely in memory, and is typically delivered and executed by a loader such as Cobalt Strike. The malware has been ported to Linux, however unlike the Windows variant the Linux variant doesn't employ Anti-Analysis measures to hinder reverse engineering. The MD5 hash of this Defray777 sample is 210f47c8f47ded8525da927710abc6ad.
Strike Defray777_aa1ddf0c	This strike sends a malware sample known as Defray777. Defray777 is an elusive family of Ransomware also known as RansomX and RansomExx that has been active since 2018. It runs entirely in memory, and is typically delivered and executed by a loader such as Cobalt Strike. The malware has been ported to Linux, however unlike the Windows variant the Linux variant doesn't employ Anti-Analysis measures to hinder reverse engineering. The MD5 hash of this Defray777 sample is aa1ddf0c8312349be614ff43e80a262f.
Strike Defray777_fcd21c6f	This strike sends a malware sample known as Defray777. Defray777 is an elusive family of Ransomware also known as RansomX and RansomExx that has been active since 2018. It runs entirely in memory, and is typically delivered and executed by a loader such as Cobalt Strike. The malware has been ported to Linux, however unlike the Windows variant the Linux variant doesn't employ Anti-Analysis measures to hinder reverse engineering. The MD5 hash of this Defray777 sample is fcd21c6fca3b9378961aa1865bee7ecb.
Strike DevOpt_391c8946	This strike sends a malware sample known as DevOpt. DevOpt is a malware backdoor that was discovered on a Russian website attempting to lure victims into downloading the malware via the promise of monetary rewards. The malware has many capabilities including the ability to enable persistence on the targeted system, steal browser credentials, grab clipboard data, and log keystrokes. The MD5 hash of this DevOpt sample is 391c894616dd0e8b372b801cbcc0a790.
Strike DevOpt_94df2e4a	This strike sends a malware sample known as DevOpt. DevOpt is a malware backdoor that was discovered on a Russian website attempting to lure victims into downloading the malware via the promise of monetary rewards. The malware has many capabilities including the ability to enable persistence on the targeted system, steal browser credentials, grab clipboard data, and log keystrokes. The MD5 hash of this DevOpt sample is 94df2e4aa0f432ef992893d7b994ce84.
Strike DevOpt_db14d40d	This strike sends a malware sample known as DevOpt. DevOpt is a malware backdoor that was discovered on a Russian website attempting to lure victims into downloading the malware via the promise of monetary rewards. The malware has many capabilities including the ability to enable persistence on the targeted system, steal browser credentials, grab clipboard data, and log keystrokes. The MD5 hash of this DevOpt sample is db14d40d780853f80b93e21e92617680.
Strike DevOpt_e42198e7	This strike sends a malware sample known as DevOpt. DevOpt is a malware backdoor that was discovered on a Russian website attempting to lure victims into downloading the malware via the promise of monetary rewards. The malware has many capabilities including the ability to enable persistence on the targeted system, steal browser credentials, grab clipboard data, and log keystrokes. The MD5 hash of this DevOpt sample is e42198e7c0647238b999a2b2133daac2.

<b>Name</b>	<b>Description</b>
Strike Dharma_09abc206	This strike sends a polymorphic malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The binary has the debug flag removed in the PE file format. The MD5 hash of this Dharma sample is 09abc206875e17ad67f96a78db948812.
Strike Dharma_0b3f26d9	This strike sends a polymorphic malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Dharma sample is 0b3f26d996dc0326a7eb88f122c21e3c.
Strike Dharma_0e54c3ae	This strike sends a malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The MD5 hash of this Dharma sample is 0e54c3ae592f46def82c6b153bb642c8.
Strike Dharma_142d30b8	This strike sends a polymorphic malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Dharma sample is 142d30b8dc05ade27ad2707988a80495.
Strike Dharma_16335b82	This strike sends a polymorphic malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The binary has a new section added in the PE file format with random contents. The MD5 hash of this Dharma sample is 16335b825864a9c678c5fc316040f5f3.

<b>Name</b>	<b>Description</b>
Strike Dharma_1fdbd39b2	<p>This strike sends a polymorphic malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The binary has random bytes appended at the end of the file. The MD5 hash of this Dharma sample is 1fdbd39b295d2935420205e385d4495cf.</p>
Strike Dharma_272d8ad1	<p>This strike sends a polymorphic malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Dharma sample is 272d8ad1848146eea7102aa423878083.</p>
Strike Dharma_2873a268	<p>This strike sends a polymorphic malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The binary has been packed using upx packer, with the default options. The MD5 hash of this Dharma sample is 2873a26848097afd920b6e6bc9375a48.</p>
Strike Dharma_3752ab93	<p>This strike sends a polymorphic malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The binary has been packed using upx packer, with the default options. The MD5 hash of this Dharma sample is 3752ab9389508c6a7f02673b89f21b52.</p>
Strike Dharma_3cdd778b	<p>This strike sends a malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The MD5 hash of this Dharma sample is 3cdd778bd9a5342996dfc5107bf11ce2.</p>

<b>Name</b>	<b>Description</b>
Strike Dharma_425913c1	This strike sends a polymorphic malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Dharma sample is 425913c1262d84268c1f03a3cde14a03.
Strike Dharma_481f271d	This strike sends a malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The MD5 hash of this Dharma sample is 481f271dc162d97f4af7453359b5be23.
Strike Dharma_48b09277	This strike sends a polymorphic malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Dharma sample is 48b09277d82efbcfa25e6dbe5dad3c5c.
Strike Dharma_6b579803	This strike sends a polymorphic malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The binary has random bytes appended at the end of the file. The MD5 hash of this Dharma sample is 6b5798035d7d54cf82271799ddd12ac.
Strike Dharma_7dfc8d87	This strike sends a malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The MD5 hash of this Dharma sample is 7dfc8d87189cce40176fc6310d08c69c.

<b>Name</b>	<b>Description</b>
Strike Dharma_8adb0b8e	This strike sends a malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The MD5 hash of this Dharma sample is 8adb0b8eaf0c51c2550bd0192d3a44ee.
Strike Dharma_96c198c5	This strike sends a malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The MD5 hash of this Dharma sample is 96c198c58939d40103a47b98431bc5de.
Strike Dharma_9a77e8be	This strike sends a malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The MD5 hash of this Dharma sample is 9a77e8be9dd41d0e9b8a77e9a2abf4de.
Strike Dharma_9b96be6c	This strike sends a malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The MD5 hash of this Dharma sample is 9b96be6c2ac05decb4b8d41469cb864e.
Strike Dharma_ad28ea90	This strike sends a polymorphic malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The binary has a new section added in the PE file format with random contents. The MD5 hash of this Dharma sample is ad28ea90c494a147758db2dfe77f5751.

<b>Name</b>	<b>Description</b>
Strike Dharma_ba67dd5a	This strike sends a malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The MD5 hash of this Dharma sample is ba67dd5ab7d6061704f2903573cec303.
Strike Dharma_c61e6887	This strike sends a polymorphic malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Dharma sample is c61e688710c50976d854b7eba9a55dea.
Strike Dharma_d154f03e	This strike sends a malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The MD5 hash of this Dharma sample is d154f03e05aa319754f1648f6257e900.
Strike Dharma_ef40a998	This strike sends a malware sample known as Dharma. Dharma also known as Crysis, is a trojanized ransomware in which the source code has been around for several years, leading to many variants being created. This availability and these variants lend to its popularity as a Ransomware as a Service model being adopted by cyber criminals. Dharma conceals itself inside the target system and encrypts files anytime they are added to the specified directory. Once the files are encrypted a ransom note is left providing the victim with email addresses to contact in order to pay for decryption. The MD5 hash of this Dharma sample is ef40a9988e3bd89190cba2bcb765b7b9.
Strike Diamond Sleet DSROLE_8b56e14e	This strike sends a malware sample known as Diamond Sleet DSROLE. DSROLE.dll is a malicious dll that has been associated with Diamond Sleet North Korean DLL search order hijacking attacks. It has been observed launching the wksprt.exe, which communicates with C2 servers. The MD5 hash of this Diamond Sleet DSROLE sample is 8b56e14e0b29ec1101accdc6a383131b.
Strike Diamond Sleet VERSION_c42f28b2	This strike sends a malware sample known as Diamond Sleet VERSION. VERSION.dll is a malicious dll that has been associated with Diamond Sleet North Korean DLL search order hijacking attacks. The dll decrypts a readme.md file that contains data that is used as a key to decrypt code in Version.dll. This code then executes and loads a Remote Access Trojan. The MD5 hash of this Diamond Sleet VERSION sample is c42f28b2851dd63928ac76d74e536ba4.

<b>Name</b>	<b>Description</b>
Strike Diavol_1aadb27c	This strike sends a malware sample known as Diavol. Diavol ransomware was first seen in 2021, but in 2022 the FBI formally linked the ransomware operation to the Trickbot group. The ransomware is known for using Asynchronous Procedure Calls with an asynchronous encryption algorithm. The ransomware also doesn't utilize obfuscation or anti-analysis techniques, but manages to make analysis difficult by storing its main routines inside bitmap images. The MD5 hash of this Diavol sample is 1aadb27c19050b903a8cf63f426db36.
Strike Diavol_76cecfea	This strike sends a malware sample known as Diavol. Diavol ransomware was first seen in 2021, but in 2022 the FBI formally linked the ransomware operation to the Trickbot group. The ransomware is known for using Asynchronous Procedure Calls with an asynchronous encryption algorithm. The ransomware also doesn't utilize obfuscation or anti-analysis techniques, but manages to make analysis difficult by storing its main routines inside bitmap images. The MD5 hash of this Diavol sample is 76cecfea2747a8b486ceb431a4e99149.
Strike Diavol_82177e34	This strike sends a malware sample known as Diavol. Diavol ransomware was first seen in 2021, but in 2022 the FBI formally linked the ransomware operation to the Trickbot group. The ransomware is known for using Asynchronous Procedure Calls with an asynchronous encryption algorithm. The ransomware also doesn't utilize obfuscation or anti-analysis techniques, but manages to make analysis difficult by storing its main routines inside bitmap images. The MD5 hash of this Diavol sample is 82177e344fdd64c38e52f97120f60350.
Strike DinodasRAT_8138f1af	This strike sends a malware sample known as DinodasRAT. DinodasRAT also known as XDealer is Linux malware that was first detected around 2021 but is still revealing variants circulating in 2024. At its core the malware is a backdoor that targets and infects Linux based architecture with the purpose of gaining and maintaining access. It does this by establishing a channel of communication back to the attacker to a C2 server that can send and execute a host of commands on the infected machine. The MD5 hash of this DinodasRAT sample is 8138f1af1dc51cde924aa2360f12d650.
Strike DinodasRAT_decd6b94	This strike sends a malware sample known as DinodasRAT. DinodasRAT also known as XDealer is Linux malware that was first detected around 2021 but is still revealing variants circulating in 2024. At its core the malware is a backdoor that targets and infects Linux based architecture with the purpose of gaining and maintaining access. It does this by establishing a channel of communication back to the attacker to a C2 server that can send and execute a host of commands on the infected machine. The MD5 hash of this DinodasRAT sample is decd6b94792a22119e1b5a1ed99e8961.
Strike Dofoil_1301e933	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typically used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is 1301e933ffd26d973e2d92726a5cb165.
Strike Dofoil_17238a77	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typically used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is 17238a77d4115a153200b352da8667e4.

<b>Name</b>	<b>Description</b>
Strike Dofoil_286321a5	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is 286321a5c27acf660cdf4305ad33a661.
Strike Dofoil_2ec070d0	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is 2ec070d0df92af50a6f873e02c0afcde.
Strike Dofoil_3584fb56	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is 3584fb561a89745f5562f34ca6d2d90e.
Strike Dofoil_3fa850b7	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is 3fa850b77ae570c62822109783db290a.
Strike Dofoil_41cbc9f1	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is 41cbc9f14ba35bc3fbc01fa373366684.
Strike Dofoil_44aad9ee	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is 44aad9eeb8af28286b332ab628d28f95.
Strike Dofoil_5b7add55	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is 5b7add55ea91cae73e7c851667f4f227.
Strike Dofoil_77bbe1ee	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is 77bbe1ee50b49407d6d05afb4ca96ff7.
Strike Dofoil_7dd17081	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is 7dd17081fb73d13df36e28ce13b0fc8c.
Strike Dofoil_945cb107	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is 945cb1078a84c7ab1871fe5d7989dc8d.

<b>Name</b>	<b>Description</b>
Strike Dofoil_a41b3582	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is a41b35821e750b19e71cdc5ece08b91f.
Strike Dofoil_abb7e72b	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is abb7e72b41ed57f9c36c429e9c07fd56.
Strike Dofoil_acdbed3a	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is acdbed3ae6e2a055308a239fe9747eea.
Strike Dofoil_b0f774c3	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is b0f774c3bbb838aaafdaedae70b4e752.
Strike Dofoil_b4f02682	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is b4f02682465301d17d8658d1c69abe6d.
Strike Dofoil_bc8169b8	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is bc8169b8f36da028c90537694d4dedf0.
Strike Dofoil_d6b15dd2	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is d6b15dd2c82446ef06feb78f18ed6435.
Strike Dofoil_e81d1b51	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is e81d1b51ee7a971cbbe4cb91f09a5d90.
Strike Dofoil_f80691f4	This strike sends a malware sample known as Dofoil. Dofoil also known as SmokeLoader is typicall used to download and execute various other malware. It has been associated with dropping and executing coin miners that mine cryptocurrency. The MD5 hash of this Dofoil sample is f80691f47500b11ae90d642583a87781.

<b>Name</b>	<b>Description</b>
Strike DoppelPaymer_2d1e555a	This strike sends a polymorphic malware sample known as DoppelPaymer. DoppelPaymer ransomware is a variant of the BitPaymer ransomware. It contains source code that can be found in both Dridex and BitPaymer. It has been delivered primarily by Dridex, however, it has also been used in numerous other methods like, malspam, botnets, exploits, etc. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this DoppelPaymer sample is 2d1e555aa68fcc2672e03c976203f96d.
Strike DoppelPaymer_2d49243c	This strike sends a malware sample known as DoppelPaymer. DoppelPaymer ransomware is a variant of the BitPaymer ransomware. It contains source code that can be found in both Dridex and BitPaymer. It has been delivered primarily by Dridex, however, it has also been used in numerous other methods like, malspam, botnets, exploits, etc. Most recently Kia Motor Company has suffered an attack from DoppelPaymer with the attackers requesting a \$27 Million dollar ransom. The MD5 hash of this DoppelPaymer sample is 2d49243c9ee70e4998362082c98e1819.
Strike DoppelPaymer_4601ec39	This strike sends a polymorphic malware sample known as DoppelPaymer. DoppelPaymer ransomware is a variant of the BitPaymer ransomware. It contains source code that can be found in both Dridex and BitPaymer. It has been delivered primarily by Dridex, however, it has also been used in numerous other methods like, malspam, botnets, exploits, etc. The binary has random bytes appended at the end of the file. The MD5 hash of this DoppelPaymer sample is 4601ec39e2934ba61651decf6d06de64.
Strike DoppelPaymer_66c11a6c	This strike sends a polymorphic malware sample known as DoppelPaymer. DoppelPaymer ransomware is a variant of the BitPaymer ransomware. It contains source code that can be found in both Dridex and BitPaymer. It has been delivered primarily by Dridex, however, it has also been used in numerous other methods like, malspam, botnets, exploits, etc. The binary has the timestamp field updated in the PE file header. The MD5 hash of this DoppelPaymer sample is 66c11a6cbbe59f2e580da1c75acd9ae8.
Strike DoppelPaymer_69061465	This strike sends a malware sample known as DoppelPaymer. DoppelPaymer ransomware is a variant of the BitPaymer ransomware. It contains source code that can be found in both Dridex and BitPaymer. It has been delivered primarily by Dridex, however, it has also been used in numerous other methods like, malspam, botnets, exploits, etc. The MD5 hash of this DoppelPaymer sample is 69061465ae5067710402c832412e2dae.
Strike DoppelPaymer_81f50e95	This strike sends a malware sample known as DoppelPaymer. DoppelPaymer ransomware is a variant of the BitPaymer ransomware. It contains source code that can be found in both Dridex and BitPaymer. It has been delivered primarily by Dridex, however, it has also been used in numerous other methods like, malspam, botnets, exploits, etc. The MD5 hash of this DoppelPaymer sample is 81f50e95bfbbe7d86229ac9592feb2f.
Strike DoppelPaymer_8c54bbe3	This strike sends a malware sample known as DoppelPaymer. DoppelPaymer ransomware is a variant of the BitPaymer ransomware. It contains source code that can be found in both Dridex and BitPaymer. It has been delivered primarily by Dridex, however, it has also been used in numerous other methods like, malspam, botnets, exploits, etc. The MD5 hash of this DoppelPaymer sample is 8c54bbe3f191a8627bfeeb4cb02634a9.

<b>Name</b>	<b>Description</b>
Strike DoppelPaymer_a6a31da6	This strike sends a polymorphic malware sample known as DoppelPaymer. DoppelPaymer ransomware is a variant of the BitPaymer ransomware. It contains source code that can be found in both Dridex and BitPaymer. It has been delivered primarily by Dridex, however, it has also been used in numerous other methods like, malspam, botnets, exploits, etc. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this DoppelPaymer sample is a6a31da60473168dc613b64c7a00fc5e.
Strike DoppelPaymer_b2a0c322	This strike sends a polymorphic malware sample known as DoppelPaymer. DoppelPaymer ransomware is a variant of the BitPaymer ransomware. It contains source code that can be found in both Dridex and BitPaymer. It has been delivered primarily by Dridex, however, it has also been used in numerous other methods like, malspam, botnets, exploits, etc. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this DoppelPaymer sample is b2a0c322572d0f5f52d92dbd336ac14f.
Strike DoppelPaymer_c9b7413e	This strike sends a malware sample known as DoppelPaymer. DoppelPaymer ransomware is a variant of the BitPaymer ransomware. It contains source code that can be found in both Dridex and BitPaymer. It has been delivered primarily by Dridex, however, it has also been used in numerous other methods like, malspam, botnets, exploits, etc. Most recently Kia Motor Company has suffered an attack from DoppelPaymer with the attackers requesting a \$27 Million dollar ransom. The MD5 hash of this DoppelPaymer sample is c9b7413e50bfb22074734d615857a6f5.
Strike Dorkbot_14cd9f53	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is 14cd9f533c23959b26089a0f3da47ebe.
Strike Dorkbot_23788137	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is 237881374e70bbe9f94bbf80a5e78580.
Strike Dorkbot_27d4b49a	This strike sends a polymorphic malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The binary file has one more imports added in the import table. The MD5 hash of this Dorkbot sample is 27d4b49aa7890f825e97fdafb1c99b2a.
Strike Dorkbot_2c8b2adb	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is 2c8b2adbe648f04b658aa9f3f4ab7ccc.

<b>Name</b>	<b>Description</b>
Strike Dorkbot_2cfa385a	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is 2cfa385a368304e57a7a3918e53401cc.
Strike Dorkbot_34f8aa91	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is 34f8aa917d5e78b3bbc66682d993e992.
Strike Dorkbot_3ec31a62	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is 3ec31a620bb155b175f1dca19d7f3abf.
Strike Dorkbot_4e3a397f	This strike sends a polymorphic malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Dorkbot sample is 4e3a397fa3e835cf6bb5ca23268cb11a.
Strike Dorkbot_4f2fcaff	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is 4f2fcaff3b068ee744b80db7474f8043.
Strike Dorkbot_535fb4c2	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is 535fb4c2c630fc80bdcbc56895528027.
Strike Dorkbot_617acc95	This strike sends a polymorphic malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Dorkbot sample is 617acc95c26c60ef3b90df8f612f4da4.
Strike Dorkbot_6ce9013f	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is 6ce9013ff2917fc2cb26fadf22df6bb9.

<b>Name</b>	<b>Description</b>
Strike Dorkbot_7866127d	This strike sends a polymorphic malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Dorkbot sample is 7866127daac6c9b5be81d2e01cc2f3f5.
Strike Dorkbot_79ac3809	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is 79ac3809d107b030fefafa02775bb26cb5.
Strike Dorkbot_89fecc6d	This strike sends a polymorphic malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The binary has random bytes appended at the end of the file. The MD5 hash of this Dorkbot sample is 89fecc6df87d3a9ec5efe7deded2560e.
Strike Dorkbot_8c5d180d	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is 8c5d180d78d43ec8c0754273f13f13d2.
Strike Dorkbot_9d763334	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is 9d763334a69c0c9ffcae3f99b4a3337d.
Strike Dorkbot_a42942f2	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is a42942f29b7e3084686d9c851ee53999.
Strike Dorkbot_a60ea31c	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is a60ea31cff0dbe199cbf6fbea03cc77d.
Strike Dorkbot_aa108570	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is aa108570154f9c81cc9e2be856f15222.

<b>Name</b>	<b>Description</b>
Strike Dorkbot_ae4bf237	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is ae4bf237bdcb56fc66d4ab3f7eefc647.
Strike Dorkbot_b8c9fdf0	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is b8c9fdf04315e62badffe4ca393de3b5.
Strike Dorkbot_b901c4d9	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is b901c4d9c76b378adb8919ae3dfa932c.
Strike Dorkbot_bec351f6	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is bec351f63f70e048f5319f8f5a386bf0.
Strike Dorkbot_c35270cf	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is c35270cfbadd4cff99be4fd906ed4b49.
Strike Dorkbot_c8e632b8	This strike sends a polymorphic malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The binary has the checksum removed in the PE file format. The MD5 hash of this Dorkbot sample is c8e632b867a715c2174bb3743d600372.
Strike Dorkbot_e2a567c0	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is e2a567c007c4446356a8b4c170eaa73d.
Strike Dorkbot_e2ffab46	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is e2ffab464f6be4b25d126ff9d1c51449.

<b>Name</b>	<b>Description</b>
Strike Dorkbot_f42c2687	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is f42c2687a386ea74defec16a76be7b85.
Strike Dorkbot_fd964c0b	This strike sends a polymorphic malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Dorkbot sample is fd964c0b89402a947716fdaddf0bf800.
Strike Dorkbot_ff68ff41	This strike sends a malware sample known as Dorkbot. Dorkbot is a worm that spreads itself through social networking sites and messaging apps. Once installed, the infected computer becomes part of a botnet, allowing the controller to control the machine remotely. The MD5 hash of this Dorkbot sample is ff68ff41082fc943576fb8412c620836.
Strike DragonEgg_1e3b46c0	This strike sends a malware sample known as DragonEgg. DragonEgg is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this DragonEgg sample is 1e3b46c0d30c4bad4cce8adec2af1154.
Strike DragonEgg_b22585b5	This strike sends a malware sample known as DragonEgg. DragonEgg is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this DragonEgg sample is b22585b5d0d5776c8914308882b23199.
Strike DragonEgg_f3796fe1	This strike sends a malware sample known as DragonEgg. DragonEgg is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this DragonEgg sample is f3796fe187560c8d93051176289e445f.
Strike DragonRank_00e3582a	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadIIS. The MD5 hash of this DragonRank sample is 00e3582a958f63378825c1bea359ab5f.

<b>Name</b>	<b>Description</b>
Strike DragonRank_07b2dd4a	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 07b2dd4a339e7ba579362de606dc9411.
Strike DragonRank_12d03e77	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 12d03e7790a534a20984ffcef967b261.
Strike DragonRank_1fdb1dd7	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 1fdb1dd742674d3939f636c3fc4b761f.
Strike DragonRank_2be57023	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 2be5702361b511c70f1aaee4b07e98bf.
Strike DragonRank_2f65873d	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 2f65873db4d6cf8ae605bdd1ee081e7a.
Strike DragonRank_405f2150	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 405f2150c05814ffbcf6f2308263707d.
Strike DragonRank_4d0e8e3c	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 4d0e8e3c38d77f80519e4a46a5a6c389.
Strike DragonRank_5996c1aa	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 5996c1aab30086c5cd1cf62cf6a9e942.
Strike DragonRank_5fc28be0	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 5fc28be056af14b1453b09f2372ee9f3.
Strike DragonRank_704437ba	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 704437baf305ea114190b087d5dc44a5.

<b>Name</b>	<b>Description</b>
Strike DragonRank_74474ccc	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 74474ccc36016b44022c0a8e90269abd.
Strike DragonRank_7968fb0f	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 7968fb0f54637e2fa745ed5410fc6886.
Strike DragonRank_7a47f695	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 7a47f695a09ff82968144858f228cd67.
Strike DragonRank_7d8c5f7d	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 7d8c5f7d684971923fc11d0033bef90d.
Strike DragonRank_7eb4d740	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 7eb4d7409446cc974ab4a62bc9a5fdf7.
Strike DragonRank_8dc8cd05	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 8dc8cd05a1a8edc53b6ef7779751bfc2.
Strike DragonRank_8f862493	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 8f862493f30b97f2c7af34bf50f9ef90.
Strike DragonRank_92cb8885	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 92cb8885aa244d4778d4e9d84c06dd39.
Strike DragonRank_930b62e5	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 930b62e51104529f9543b4fe96c98bda.
Strike DragonRank_9363fa01	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 9363fa01a791889ec72655717edee6c2.

<b>Name</b>	<b>Description</b>
Strike DragonRank_9b032d7e	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 9b032d7edd2deeeeb662b3172386970b.
Strike DragonRank_9d56ce6d	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is 9d56ce6db4868af796fd82f01b3fe6ef.
Strike DragonRank_a043443a	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is a043443af3021d1f6b58ce87ba264f4d.
Strike DragonRank_a17ea49b	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is a17ea49b998508ef9be7a087c33784bc.
Strike DragonRank_a57a7862	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is a57a78624756d9d6a8929476d6685bc9.
Strike DragonRank_ac035c9b	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is ac035c9b4b73dc3a80fc93ce976c4889.
Strike DragonRank_ad7e5df7	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is ad7e5df7a54b38176476cdc545129d41.
Strike DragonRank_b5848af3	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is b5848af3dae4370928e3adc091facbc2.
Strike DragonRank_b779d9ef	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is b779d9efc1e00e2626e9942d9a065666.
Strike DragonRank_d6f3fef9	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is d6f3fef9e39b7b7f0e7b2d29f6cbb213.

<b>Name</b>	<b>Description</b>
Strike DragonRank_d7717cd1	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is d7717cd15c28d31674776242d531d0c2.
Strike DragonRank_e9194bd2	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is e9194bd20e9bd6f6f5e572796514b285.
Strike DragonRank_e99b6437	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is e99b6437f572927ea2e4746dfb542e37.
Strike DragonRank_f2047fae	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is f2047fae637746ef4d7a4d2f81c2894f.
Strike DragonRank_f3524e85	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is f3524e85359ddca920f1600125499ca8.
Strike DragonRank_f9b7a389	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is f9b7a389f995c7f01c37351afc457fa4.
Strike DragonRank_fae95f61	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is fae95f61b4970c3769b7d8dffcc1b8dd.
Strike DragonRank_fb5dffda	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is fb5dffda1bbbc25318c9fd247733fbe.
Strike DragonRank_fd24ad04	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is fd24ad0498a206d322bf7605d13be1bf.
Strike DragonRank_fe67d584	This strike sends a malware sample known as DragonRank. DragonRank is malware that targets web application services and uses them to deploy a web shell to collect system information and launch additional malware like PlugX and BadiIIS. The MD5 hash of this DragonRank sample is fe67d584f11a0ca94a0d69e2ff123fda.

<b>Name</b>	<b>Description</b>
Strike DuneQuixote_00130e1e	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 00130e1e7d628c8b5e2f9904ca959cd7.
Strike DuneQuixote_0d740972	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 0d740972c3dff09c13a5193d19423da1.
Strike DuneQuixote_0fbe82d	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 0fbe82d2c8d52ac912d698bb8b25abc.
Strike DuneQuixote_135abd6f	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 135abd6f35721298cc656a29492be255.
Strike DuneQuixote_1bba771b	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 1bba771b9a32f0aada6eaee64643673a.
Strike DuneQuixote_258b7f20	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 258b7f20db8b927087d74a9d6214919b.
Strike DuneQuixote_3aaaf7f7f	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 3aaaf7f7f0a42a1cf0a0f6c61511978d7.

<b>Name</b>	<b>Description</b>
Strike DuneQuixote_3cc77c18	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 3cc77c18b4d1629b7658afbf4175222c.
Strike DuneQuixote_4324cb72	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 4324cb72875d8a62a210690221cdc3f9.
Strike DuneQuixote_450e5896	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 450e589680e812ffb732f7e889676385.
Strike DuneQuixote_48c8e8cc	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 48c8e8cc189eeef04a55ecb021f9e6111.
Strike DuneQuixote_4f29f977	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 4f29f977e786b2f7f483b47840b9c19d.
Strike DuneQuixote_5200fa68	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 5200fa68b6d40bb60d4f097b895516f0.
Strike DuneQuixote_56d5589e	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 56d5589e0d6413575381b1f3c96aa245.

<b>Name</b>	<b>Description</b>
Strike DuneQuixote_5759acc8	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 5759acc816274d38407038c091e56a5c.
Strike DuneQuixote_5a04d906	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 5a04d9067b8cb6bcb916b59dcf53bed3.
Strike DuneQuixote_5e85dc7c	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 5e85dc7c6969ce2270a06184a8c8e1da.
Strike DuneQuixote_606fdee7	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 606fdee74ad70f76618007d299adb0a4.
Strike DuneQuixote_6cfec4bd	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 6cfec4bdcacf7f99535ee61a0ebae5dc.
Strike DuneQuixote_71a8b4b8	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 71a8b4b8d9861bf9ac6bd4b0a60c3366.
Strike DuneQuixote_72c4d9bc	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 72c4d9bc1b59da634949c555b2a594b1.

<b>Name</b>	<b>Description</b>
Strike DuneQuixote_7b9e85af	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 7b9e85afa89670f46f884bb3bce262b0.
Strike DuneQuixote_828335d0	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 828335d067b27444198365fac30aa6be.
Strike DuneQuixote_84ae9222	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 84ae9222c86290bf585851191007ba23.
Strike DuneQuixote_91472c23	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 91472c23ef5e8b0f8dda5fa9ae9afa94.
Strike DuneQuixote_996c4f78	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 996c4f78a13a8831742e86c052f19c20.
Strike DuneQuixote_9b991229	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 9b991229fe1f5d8ec6543b1e5ae9beb4.
Strike DuneQuixote_9d20cc7a	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is 9d20cc7a02121b515fd8f16b576624ef.

<b>Name</b>	<b>Description</b>
Strike DuneQuixote_a0802a78	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is a0802a787537de1811a81d9182be9e7c.
Strike DuneQuixote_a4011d2e	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is a4011d2e4d3d9f9fe210448dd19c9d9a.
Strike DuneQuixote_abf16e31	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is abf16e31deb669017e10e2cb8cc144c8.
Strike DuneQuixote_b0e19a9f	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is b0e19a9fd168af2f7f6cf997992b1809.
Strike DuneQuixote_c7076351	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is c70763510953149fb33d06bef160821c.
Strike DuneQuixote_cc05c7be	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is cc05c7bef5cff67bc74fda2fc96ddf7b.
Strike DuneQuixote_cf4bef85	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is cf4bef8537c6397ba07de7629735eb4e.

<b>Name</b>	<b>Description</b>
Strike DuneQuixote_db786b77	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is db786b773cd75483a122b72fdc392af6.
Strike DuneQuixote_f151be4e	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is f151be4e882352ec42a336ca6bff7e3d.
Strike DuneQuixote_f1b6aa55	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is f1b6aa55ba3bb645d3fde78abda984f3.
Strike DuneQuixote_f3988b8a	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is f3988b8aaaa8c6a9ec407cf5854b0e3b.
Strike DuneQuixote_fb2b916e	This strike sends a malware sample known as DuneQuixote. This malware sample is known as DonQuixote. It is part of a campaign that targets entities in the Middle East. It uses memory-only implants and droppers to deploy an array of tools to maintain stealth and establish persistence on the system. Once activated the malware awaits C2 commands to enable it to perform file upload/download and command execution tasks. The MD5 hash of this DuneQuixote sample is fb2b916e44abddd943015787f6a8dc35.
Strike Earth Alux_0214e371	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 0214e37107c84a580288c5ffc5706d01.
Strike Earth Alux_10a309d6	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 10a309d6789c7763ec207961ac088689.

<b>Name</b>	<b>Description</b>
Strike Earth Alux_1cffc6f2	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 1cffc6f22f9837062f499570bcc393d3.
Strike Earth Alux_1fc97fdc	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 1fc97fdc9d87a4c6352d5dd1a27b2bea.
Strike Earth Alux_27d87879	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 27d878799cd23d43e93f44d4a2ce6792.
Strike Earth Alux_32a1e497	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 32a1e497b981dbbf78a6a6b6efe353a7.
Strike Earth Alux_3f73109e	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 3f73109e24a3d8fbebb8be5b4eafc2c2.
Strike Earth Alux_3fecff30	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 3fecff305be731c8e4a82ee427a244e6.
Strike Earth Alux_61d72565	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 61d72565e936eb04b734914e26223865.

<b>Name</b>	<b>Description</b>
Strike Earth Alux_63032105	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 63032105c83f2b904aba1926a05c7353.
Strike Earth Alux_6351e7f4	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 6351e7f4c55484423154abe318a706ec.
Strike Earth Alux_635a18a9	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 635a18a9f153c8853b5f9dd2d27a0892.
Strike Earth Alux_6937c923	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 6937c923ca4946748694179f1e39433b.
Strike Earth Alux_6e1fd4b0	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 6e1fd4b0bd83c99ddba761b9d9ba2891.
Strike Earth Alux_7a7bc7b5	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 7a7bc7b5187d3b0f05986567027d29b3.
Strike Earth Alux_7e18911b	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 7e18911b416a928fe64574468c5dee98.

<b>Name</b>	<b>Description</b>
Strike Earth Alux_9e3f1471	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is 9e3f14717e8dcf9745c3083d1ac3952d.
Strike Earth Alux_b07d35c7	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is b07d35c7c74df623829da5be1d76068a.
Strike Earth Alux_b821f9d2	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is b821f9d2364b4c457a097f11042212c6.
Strike Earth Alux_ce307882	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is ce3078820889e28e497b43c6f6103689.
Strike Earth Alux_d0394b2f	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is d0394b2f7ae865397f3ce73d8b60db23.
Strike Earth Alux_d65a43c6	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is d65a43c6c6ae3281ea8ff301743d7251.
Strike Earth Alux_e2865d48	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is e2865d480ab49b6b7e25cf19310509c9.

<b>Name</b>	<b>Description</b>
Strike Earth Alux_e849bf33	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is e849bf3328b1a0a7834d420cb5d79df7.
Strike Earth Alux_ef2016bd	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is ef2016bd438ad1026733ad00e047c385.
Strike Earth Alux_f3f02c5a	This strike sends a malware sample known as Earth Alux. This malware sample is part of the Earth Alux APT group cyberespionage attacks that were observed in the Asian Pacific region. Earth Alux utilizes malware web shells like GODZILLA to implant backdoors like VARGEIT. Another component to the attack is the RAILLOAD loader tool which is executed via DLL side loading. This sample is part of this attack chain. The MD5 hash of this Earth Alux sample is f3f02c5adea6974c421080c19d0bf34f.
Strike EddieStealer_20745dc4	This strike sends a malware sample known as EddieStealer. EddieStealer is an info stealer malware written in Rust. This malware has been leveraged in campaigns that utilize fake captcha pages to trigger a powershell script to download and execute the EddieStealer payload. The MD5 hash of this EddieStealer sample is 20745dc4d048f67e0b62aca33be80283.
Strike EddieStealer_4776ff45	This strike sends a malware sample known as EddieStealer. EddieStealer is an info stealer malware written in Rust. This malware has been leveraged in campaigns that utilize fake captcha pages to trigger a powershell script to download and execute the EddieStealer payload. The MD5 hash of this EddieStealer sample is 4776ff459c881a5b876da396f7324c64.
Strike EddieStealer_6342c055	This strike sends a malware sample known as EddieStealer. EddieStealer is an info stealer malware written in Rust. This malware has been leveraged in campaigns that utilize fake captcha pages to trigger a powershell script to download and execute the EddieStealer payload. The MD5 hash of this EddieStealer sample is 6342c05504154d958af852b3ea265afc.
Strike EddieStealer_673c9988	This strike sends a malware sample known as EddieStealer. EddieStealer is an info stealer malware written in Rust. This malware has been leveraged in campaigns that utilize fake captcha pages to trigger a powershell script to download and execute the EddieStealer payload. The MD5 hash of this EddieStealer sample is 673c99885c030506fff25f1c23ae06b8.
Strike EddieStealer_6cc65422	This strike sends a malware sample known as EddieStealer. EddieStealer is an info stealer malware written in Rust. This malware has been leveraged in campaigns that utilize fake captcha pages to trigger a powershell script to download and execute the EddieStealer payload. The MD5 hash of this EddieStealer sample is 6cc654225172ef70a189788746ccb445.

<b>Name</b>	<b>Description</b>
Strike EddieStealer_a034dbfd	This strike sends a malware sample known as EddieStealer. EddieStealer is an info stealer malware written in Rust. This malware has been leveraged in campaigns that utilize fake captcha pages to trigger a powershell script to download and execute the EddieStealer payload. The MD5 hash of this EddieStealer sample is a034dbfd78b95e121d7603626f19f2a7.
Strike EddieStealer_c21c7aac	This strike sends a malware sample known as EddieStealer. EddieStealer is an info stealer malware written in Rust. This malware has been leveraged in campaigns that utilize fake captcha pages to trigger a powershell script to download and execute the EddieStealer payload. The MD5 hash of this EddieStealer sample is c21c7aac8d0c9e72a45f2cef7a5f6455.
Strike EddieStealer_c8c3e658	This strike sends a malware sample known as EddieStealer. EddieStealer is an info stealer malware written in Rust. This malware has been leveraged in campaigns that utilize fake captcha pages to trigger a powershell script to download and execute the EddieStealer payload. The MD5 hash of this EddieStealer sample is c8c3e658881593d798da07a1b80f250c.
Strike Elephant Dropper_06124da5	This strike sends a malware sample known as Elephant Dropper. SaintBear also known as UAC-0056 or UNC2589 is a malicious threat actor group that has been tied to the WhisperGate and WhisperKill attacks against Ukraine. Elephant is a campaign that begins as a phishing email that contains a macro embedded Microsoft Excel document that drops a Microsoft signed Elephant Dropper named 'Base-Update.exe' written in Golang. The dropper decodes a C2 address and retrieves the Elephant Downloader named 'java-sdk.exe'. The downloader, also written in Golang, retrieves the final stages of the attack the Elephant Implant and the Elephant Client. The Implant named 'oracle-java.exe' also known as GrimPlant backdoor allows the malware to communicate to the C2 via RPC requests. The Elephant Client named 'microsoft-cortana.exe' also known as Graph Steel backdoor steals user information like Wifi data and browser credentials. This sample is the Elephant Dropper. The MD5 hash of this Elephant Dropper sample is 06124da5b4d6ef31dbfd7a6094fc52a6.
Strike Embargo_0b190460	This strike sends a malware sample known as Embargo. Embargo is ransomware that is delivered as a part of a Rust-based toolkit. This toolkit consists of a loader, EDR killer, MDeployer and MS4Killer. Embargo utilizes Rust to allow for cross platform compilation. The group provides Ransomware-as-a-Service and utilizes double extortion as well by threatening to publish stolen data to leak sites. The MD5 hash of this Embargo sample is 0b1904602a90ed190066095f29a3f92a.
Strike Embargo_5d55fb70	This strike sends a malware sample known as Embargo. Embargo is ransomware that is delivered as a part of a Rust-based toolkit. This toolkit consists of a loader, EDR killer, MDeployer and MS4Killer. Embargo utilizes Rust to allow for cross platform compilation. The group provides Ransomware-as-a-Service and utilizes double extortion as well by threatening to publish stolen data to leak sites. The MD5 hash of this Embargo sample is 5d55fb708834d5ccde15d36554ea63e8.

<b>Name</b>	<b>Description</b>
Strike Embargo_dbf8fe8b	This strike sends a malware sample known as Embargo. Embargo is ransomware that is delivered as a part of a Rust-based toolkit. This toolkit consists of a loader, EDR killer, MDeployer and MS4Killer. Embargo utilizes Rust to allow for cross platform compilation. The group provides Ransomware-as-a-Service and utilizes double extortion as well by threatening to publish stolen data to leak sites. The MD5 hash of this Embargo sample is dbf8fe8bde46ead1bc550a03ad4a3f74.
Strike Embargo_f0ac3999	This strike sends a malware sample known as Embargo. Embargo is ransomware that is delivered as a part of a Rust-based toolkit. This toolkit consists of a loader, EDR killer, MDeployer and MS4Killer. Embargo utilizes Rust to allow for cross platform compilation. The group provides Ransomware-as-a-Service and utilizes double extortion as well by threatening to publish stolen data to leak sites. The MD5 hash of this Embargo sample is f0ac3999d4020cd051052a0627a2056d.
Strike Emotet_007a2eae	This strike sends a malware sample known as Emotet. Emotet is one of the most distributed active malware families today. It is modular malware in that it can deliver various payloads. Emotet often comes from Microsoft Office document macros, that is sent with malicious emails. The MD5 hash of this Emotet sample is 007a2eae29bc5bfa2eec17ae8104f61e.
Strike Emotet_0333ae5d	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 0333ae5de2a0d61a36fcdfbbb28e977.
Strike Emotet_060060f9	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Emotet sample is 060060f91dfd30f989bb1e9704addfee.
Strike Emotet_061262ce	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 061262ce488b46d0252fdc21d3d4bc7f.
Strike Emotet_07697f8d	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 07697f8df7d43a8417d53d493c78190b.
Strike Emotet_07a132c1	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 07a132c19d1feaecd623e3c271134af2.

<b>Name</b>	<b>Description</b>
Strike Emotet_087117e5	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 087117e537d3c15a3d74a240e07c632c.
Strike Emotet_09a87f23	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 09a87f23ccd5a5459bfb443faffd76f1.
Strike Emotet_0ae74d12	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 0ae74d12e881daf1de8c05d48a6f5867.
Strike Emotet_0b422cc0	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 0b422cc0719a274d2da0e23d68091b41.
Strike Emotet_1034405a	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary has the debug flag removed in the PE file format. The MD5 hash of this Emotet sample is 1034405a7a4f24541844597170e8467f.
Strike Emotet_10717df4	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 10717df40000d7f0575ccefa8ef064c5.
Strike Emotet_193e710f	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 193e710f76dbb30bf8b0fc0168a13a3d.
Strike Emotet_1a6995e8	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 1a6995e8668456e77f554af0dc360b7f.

<b>Name</b>	<b>Description</b>
Strike Emotet_1cf9f32e	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Emotet sample is 1cf9f32e7c95143df2125a20cb8d5ff.
Strike Emotet_1d6b71de	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 1d6b71ded16731da9f674977017a1b46.
Strike Emotet_1df512f0	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 1df512f03d79ca0a67d084914fb84cc1.
Strike Emotet_2082c7d3	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 2082c7d38e1a7296dd6c49582d1c5fd0.
Strike Emotet_20ad8937	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 20ad893754a3df823fa368fe84e51a8a.
Strike Emotet_212ede8e	This strike sends a malware sample known as Emotet. Emotet is one of the most distributed active malware families today. It is modular malware in that it can deliver various payloads. Emotet often comes from Microsoft Office document macros, that is sent with malicious emails. The MD5 hash of this Emotet sample is 212ede8ee978a5979b17d9d68a497d10.
Strike Emotet_22d632bd	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary has the checksum removed in the PE file format. The MD5 hash of this Emotet sample is 22d632bddf6ea7f623a15414b9b63669.
Strike Emotet_23b8353f	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 23b8353fa069bd2e95cb726e0382b674.

<b>Name</b>	<b>Description</b>
Strike Emotet_23fe2956	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 23fe29563e7cae4a432566c693bbc9ca.
Strike Emotet_24e3a9e0	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary file has one more imports added in the import table. The MD5 hash of this Emotet sample is 24e3a9e0e4b9139977cd4776c73edfc3.
Strike Emotet_270d4a7c	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 270d4a7cd0dc8f8aa84619dbcfdb13.
Strike Emotet_2a0d4de9	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 2a0d4de98de7038d61185c4fcfa5e0b6.
Strike Emotet_2c8fd0a8	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 2c8fd0a8e770e5944ae20aa5c3f45e1a.
Strike Emotet_2ff6f44d	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 2ff6f44d228c8fc133d53f7002552b2a.
Strike Emotet_31457286	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 314572861360db51d2d49afb464d4a72.
Strike Emotet_35989c84	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary has been packed using upx packer, with the default options. The MD5 hash of this Emotet sample is 35989c844a2a70f6965b8a0559af7455.

<b>Name</b>	<b>Description</b>
Strike Emotet_3d0b6c5c	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 3d0b6c5cb6699ab80d09a35dc8ff7195.
Strike Emotet_3da1215c	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 3da1215cabb6bb88d9a1432f78df501e.
Strike Emotet_3da98789	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 3da9878997705570052d1a3ae3270671.
Strike Emotet_3e9f7bc3	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 3e9f7bc31ba3adb2638de4ebec51df91.
Strike Emotet_3eb9a044	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 3eb9a044ac8c8f5685c9b43deb4c8755.
Strike Emotet_4247302f	This strike sends a malware sample known as Emotet. Emotet is one of the most distributed active malware families today. It is modular malware in that it can deliver various payloads. Emotet often comes from Microsoft Office document macros, that is sent with malicious emails. The MD5 hash of this Emotet sample is 4247302ff7876d70434aa55bf65fe7e1.
Strike Emotet_4249fe0b	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 4249fe0bca2c3b5b5cb48d42814cefbb.
Strike Emotet_42a50d33	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 42a50d33c68d817c700f1bbbb79b6c83.
Strike Emotet_43464293	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 4346429384893a6f9d4a25e2abae8bc2.

<b>Name</b>	<b>Description</b>
Strike Emotet_44fff49e	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 44fff49e71649e36c9f873289f144afb.
Strike Emotet_46d69f8e	This strike sends a malware sample known as Emotet. Emotet is one of the most distributed active malware families today. It is modular malware in that it can deliver various payloads. Emotet often comes from Microsoft Office document macros, that is sent with malicious emails. The MD5 hash of this Emotet sample is 46d69f8e1deebb60b276e62047b7ea8e.
Strike Emotet_498307c2	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Emotet sample is 498307c24d3857a0300974df6787faf0.
Strike Emotet_4a17b559	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 4a17b55969581f2b7a69e1f26d9a88e9.
Strike Emotet_4b9584ee	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 4b9584eec0429d422bca4eb61e3acd5e.
Strike Emotet_4c5d5d22	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Emotet sample is 4c5d5d22aeeec6ef3e98136bd9d3e20ec.
Strike Emotet_4db1818e	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 4db1818e989157ec2477fa8587d69033.
Strike Emotet_4e27e219	This strike sends a malware sample known as Emotet. Emotet is one of the most distributed active malware families today. It is modular malware in that it can deliver various payloads. Emotet often comes from Microsoft Office document macros, that is sent with malicious emails. The MD5 hash of this Emotet sample is 4e27e2197bda5e1318eb13ea06b18205.

<b>Name</b>	<b>Description</b>
Strike Emotet_501b6b39	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 501b6b3922ce1d5b7d555a429404e95b.
Strike Emotet_51e25f03	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 51e25f0318a7870bafa3ca4e6e419024.
Strike Emotet_52316a19	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 52316a19d6a9ce260ca3e63a56168de8.
Strike Emotet_524e824a	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 524e824ac17c816c0bd50ffae623507.
Strike Emotet_544de53a	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 544de53a55edbad56db93c07002f7ec0.
Strike Emotet_553e53c9	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 553e53c975d2ff6346302210a2145b14.
Strike Emotet_5601cc2b	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 5601cc2bfc8ea64170bec29817fe2c5a.
Strike Emotet_56b39a66	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 56b39a662e0b6bbb1ff4c2698a909407.
Strike Emotet_571ad3e0	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 571ad3e0d627ea0b6acb95f9e35e0661.

<b>Name</b>	<b>Description</b>
Strike Emotet_57674369	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 57674369f83c58d391eff88877f0fce2.
Strike Emotet_577a8dcc	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 577a8dcc160796201bf93e2a829edbee.
Strike Emotet_5870c54f	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary has the checksum removed in the PE file format. The MD5 hash of this Emotet sample is 5870c54fd187968c3c347703bd59ab1d.
Strike Emotet_5a53c95e	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 5a53c95ec818e32cec3e647a41420fb.
Strike Emotet_5ba6287e	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 5ba6287e4ade00a379c143507cb72822.
Strike Emotet_5c8b4114	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 5c8b41146f1e86614cd33ca08a60b701.
Strike Emotet_5dba15ae	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 5dba15aec0800e03cac012455c47504c.
Strike Emotet_5e15ca4c	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 5e15ca4c570e54853e6663c0783b4f51.

<b>Name</b>	<b>Description</b>
Strike Emotet_5ee3d0bb	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 5ee3d0bb7042031785c185e3402f8298.
Strike Emotet_61214202	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 61214202b2cf47ac495e9a26dd967ab1.
Strike Emotet_6213f591	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 6213f5911227d1c1a3e16c44734ecd61.
Strike Emotet_62ff36ab	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Emotet sample is 62ff36ab8ff180c7e849bf2b70cbe858.
Strike Emotet_64c5ac3e	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 64c5ac3e5f42ff74c1a174513517e894.
Strike Emotet_6828a7a0	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 6828a7a021d602c0866f83ad82404ab2.
Strike Emotet_686123fc	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 686123fcce69aac06a9d4d3aa0c9a84b.
Strike Emotet_68b36e7e	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 68b36e7efd2a6f2b24893650e30e15ea.

<b>Name</b>	<b>Description</b>
Strike Emotet_68d5c1d0	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 68d5c1d02f043dce930ccc33681d3b32.
Strike Emotet_69833f53	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 69833f53d536888fc2c2d533b33c571d.
Strike Emotet_699bd905	This strike sends a malware sample known as Emotet. Emotet is one of the most distributed active malware families today. It is modular malware in that it can deliver various payloads. Emotet often comes from Microsoft Office document macros, that is sent with malicious emails. The MD5 hash of this Emotet sample is 699bd9053663bbdeb39df9d6f4f2b483.
Strike Emotet_69db12ac	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 69db12acb99d3b6e65ba54df9d15f264.
Strike Emotet_6a874f58	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 6a874f582aa5cf1c75a52c5ed8e8a92.
Strike Emotet_6b7e027f	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 6b7e027f357b49fbff377dd6981d3873.
Strike Emotet_6b8e4dc4	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary has been packed using upx packer, with the default options. The MD5 hash of this Emotet sample is 6b8e4dc413f5f37594d193dda39efe9.
Strike Emotet_6bd3cdbf	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 6bd3cdbf9a8d0125e295c8c34f94b3ec.

<b>Name</b>	<b>Description</b>
Strike Emotet_6c65c65f	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 6c65c65f33a2720ad29bf19bc869d75d.
Strike Emotet_6c8d926b	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 6c8d926bafb7ea766b7d52ad9c00edca.
Strike Emotet_6d3c405e	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 6d3c405e03ea38e977f5473bbbdd123e.
Strike Emotet_6d7e080c	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 6d7e080c1ffd4194b7620d26cc77f6f3.
Strike Emotet_6ffeca7b	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 6ffeca7b3b65f684033a76e1b24b85df.
Strike Emotet_70601b3d	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 70601b3dfc803b1f79e85989da8354ff.
Strike Emotet_74e9ae66	This strike sends a malware sample known as Emotet. Emotet is one of the most distributed active malware families today. It is modular malware in that it can deliver various payloads. Emotet often comes from Microsoft Office document macros, that is sent with malicious emails. The MD5 hash of this Emotet sample is 74e9ae66b4029ce403ef9a76d2dd1ec4.
Strike Emotet_77157bac	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 77157bac82df74cfbc5010f637893c51.
Strike Emotet_777fb72a	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 777fb72a680ea2ccb37c6d98d4ae427c.

<b>Name</b>	<b>Description</b>
Strike Emotet_77f8dc9a	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 77f8dc9a261d51a58f653f990d0547b5.
Strike Emotet_7e8708c2	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 7e8708c2095b5b3bd833f96fc20e4dc7.
Strike Emotet_7e971bb3	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 7e971bb31ffe50dd3ed63f388881229d.
Strike Emotet_82c1170c	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 82c1170c14c34f977c5a1d7ff26da6f1.
Strike Emotet_86c8733c	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 86c8733c7bbafc20abc4d91eab8faca5.
Strike Emotet_87ef8852	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 87ef88526bb7178f95a43099a8225dd0.
Strike Emotet_882439a0	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Emotet sample is 882439a02af524719ca974b0925d42c9.
Strike Emotet_88cc1c60	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 88cc1c601c28901033abec4389854884.

<b>Name</b>	<b>Description</b>
Strike Emotet_8cdace86	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 8cdace8642fe8dd4c649bf6a9dc6d632.
Strike Emotet_8dde30a4	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 8dde30a43ef9d22ec22c1d7bcec31b20.
Strike Emotet_90198f7c	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 90198f7cc5a722554e939f84d8dcb97d.
Strike Emotet_90e32b98	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 90e32b98e17eead923b4ef0159deb1fc.
Strike Emotet_91adac33	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 91adac33b6d93c6991e2cfb4530a6464.
Strike Emotet_93835135	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 938351350f6df43ec1aa024352175807.
Strike Emotet_97e77c7d	This strike sends a malware sample known as Emotet. Emotet is one of the most distributed active malware families today. It is modular malware in that it can deliver various payloads. Emotet often comes from Microsoft Office document macros, that is sent with malicious emails. The MD5 hash of this Emotet sample is 97e77c7db614b3304ea6ef7a598697fb.
Strike Emotet_9826fccb	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 9826fccb9fe8ccb6e3486b997fa65a2e.
Strike Emotet_987e06f9	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 987e06f9676abb7ea38b10912c649637.

<b>Name</b>	<b>Description</b>
Strike Emotet_9a45c567	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 9a45c5675acd860cd45950be5f300546.
Strike Emotet_9a8f5a8c	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 9a8f5a8cd29c49c49890edcae1f3a2d9.
Strike Emotet_9aa171b7	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 9aa171b75821e33cfda05772d22f6930.
Strike Emotet_9b638d31	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 9b638d312db2f61f37c5aa02b136f7c4.
Strike Emotet_9be366b8	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Emotet sample is 9be366b807f0599182773345a95fa466.
Strike Emotet_9c270b9a	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 9c270b9a074f8e866af32a369e65aa87.
Strike Emotet_9db82b4e	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is 9db82b4e3957bf1d62d7526821b12d62.
Strike Emotet_a047e8bc	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is a047e8bc82f34dffefd1748eee7a7160.

<b>Name</b>	<b>Description</b>
Strike Emotet_a0c0c876	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is a0c0c876217f30ee39fd06de0fc8f57.
Strike Emotet_a2935c23	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is a2935c23622f35302f4b43121d62727b.
Strike Emotet_a30ba05c	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is a30ba05c61d91c62087ef7bbbb054f50.
Strike Emotet_a6ae4aaf	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is a6ae4aaf85b21a4b811504d50054bb13.
Strike Emotet_aa748718	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is aa748718088e7bb3da20377603dd39a9.
Strike Emotet_ab3cfa53	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is ab3cfa539864768c3f40d148911a6dce.
Strike Emotet_ab6e5de9	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is ab6e5de935d30d6ecedccf1296cd4ba8.
Strike Emotet_ac1464a7	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is ac1464a7af3438caeccc8d4bc797fc59.
Strike Emotet_ae7bec88	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is ae7bec88c8bf1ce8c445ec160df957fa.

<b>Name</b>	<b>Description</b>
Strike Emotet_afa31947	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is afa319478129ca124eb094c85053c3b5.
Strike Emotet_b4c7c4ce	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is b4c7c4ce08e8a2e6e6890fc57c944594.
Strike Emotet_b6c73e75	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is b6c73e75e309ca965c41e0d063224add.
Strike Emotet_b9c7ae5b	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is b9c7ae5b0efad2fb73c47cb81c52d729.
Strike Emotet_bbcb2ae7	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is bbcb2ae776fc56d292f741c4de5394fc.
Strike Emotet_bd2970ad	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is bd2970ad4cc61e3c623b9d9d54ebbad5.
Strike Emotet_bd50c433	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is bd50c4330c3b2288a7fc014c14eab7e6.
Strike Emotet_bd562cd9	This strike sends a malware sample known as Emotet. Emotet is one of the most distributed active malware families today. It is modular malware in that it can deliver various payloads. Emotet often comes from Microsoft Office document macros, that is sent with malicious emails. The MD5 hash of this Emotet sample is bd562cd9ad0134eb4ad2600ff5f2a66e.
Strike Emotet_bd57c86b	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is bd57c86b7951578d3a4a163b6d6da6c5.

<b>Name</b>	<b>Description</b>
Strike Emotet_c0c2630f	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is c0c2630f15827788f864b51ad4e66f2e.
Strike Emotet_c3b7af5b	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is c3b7af5b876b04e9e246d9e4e727807d.
Strike Emotet_c703787a	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is c703787ab240e6a6959b267c71b4927d.
Strike Emotet_c73019b6	This strike sends a malware sample known as Emotet. Emotet is one of the most distributed active malware families today. It is modular malware in that it can deliver various payloads. Emotet often comes from Microsoft Office document macros, that is sent with malicious emails. The MD5 hash of this Emotet sample is c73019b6b6b46c63f6a45c38b8c2ebbf.
Strike Emotet_c730e1c3	This strike sends a malware sample known as Emotet. Emotet is one of the most distributed active malware families today. It is modular malware in that it can deliver various payloads. Emotet often comes from Microsoft Office document macros, that is sent with malicious emails. The MD5 hash of this Emotet sample is c730e1c3cf2e54af08072778a7fd6f41.
Strike Emotet_c7962586	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is c7962586a21f367da0b957cb181e83e5.
Strike Emotet_ca12d7e7	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is ca12d7e789a88651cb742f0f5dc41e11.
Strike Emotet_caeb9d29	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is caeb9d29e22f04ae4c66b039c8fd650c.
Strike Emotet_caf8cac0	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is caf8cac0abd6e928a6de6e4d618ca5b2.

<b>Name</b>	<b>Description</b>
Strike Emotet_ce27e41e	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is ce27e41e75ad21b3d7ffbcca40a2e989.
Strike Emotet_cefea1e3	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is cefea1e3ce55f515d59c388b3ec1407c.
Strike Emotet_cf646280	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is cf6462805439b4d988e6a1f3c0c5ac32.
Strike Emotet_cf8f5f43	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is cf8f5f43d692d6a2ab060a4b7ca14246.
Strike Emotet_d206510e	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is d206510eee9c015251b40bdb0b3af3c5.
Strike Emotet_d35d7837	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is d35d78375112398893a1029368872902.
Strike Emotet_d4e7d65b	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is d4e7d65bfdcdc3a4330bbb70b4ceefef.
Strike Emotet_d8df851b	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is d8df851b1507deccf075c7838edb9a40.
Strike Emotet_d9cce403	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is d9cce403cd6642af5baaf58e128bb583.

<b>Name</b>	<b>Description</b>
Strike Emotet_dbf37811	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is dbf378111040a4cdbfea91d8743c332d.
Strike Emotet_ddb5f7ed	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is ddb5f7edb95707c0fb6d0d53907c051a.
Strike Emotet_debd3b52	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is debd3b52b96f9903d5b877d39aebe3f4.
Strike Emotet_ded35670	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is ded35670bda388674fbdf6cfb90d51c5.
Strike Emotet_df080c0c	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is df080c0cfa03ff1444dd310bbeec1fe4.
Strike Emotet_e1b3e16b	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is e1b3e16bd44ea7957e00bbf5bfbd92d6.
Strike Emotet_e1c97191	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is e1c97191eae9b1537778fc88220c44ed.
Strike Emotet_e3740306	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is e37403061d0fc0c796f6d107b7c79492.
Strike Emotet_e45b696e	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is e45b696e11a9b63bc735dac36e2e81f3.

<b>Name</b>	<b>Description</b>
Strike Emotet_e4de4b24	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is e4de4b24bf98b3af0b5732a10e5a159f.
Strike Emotet_e73d0b88	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is e73d0b8841158cc52a3f52c1162b4f1a.
Strike Emotet_e7902137	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is e79021377681dd21a34ea9a4d33dfbf6.
Strike Emotet_eb1db6d0	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is eb1db6d06bccf86bc8d8240cda956938.
Strike Emotet_ef389a78	This strike sends a malware sample known as Emotet. Emotet is one of the most distributed active malware families today. It is modular malware in that it can deliver various payloads. Emotet often comes from Microsoft Office document macros, that is sent with malicious emails. The MD5 hash of this Emotet sample is ef389a7806af11a628bcce9be3897f72.
Strike Emotet_ef569bb3	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary has been packed using upx packer, with the default options. The MD5 hash of this Emotet sample is ef569bb3d1670f0a4cbed0b8be1475fb.
Strike Emotet_f2110b23	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is f2110b231bf6209e17b59f232ca21b94.
Strike Emotet_f2a4366a	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is f2a4366aa466a11ccf4ebff87b275e17.

<b>Name</b>	<b>Description</b>
Strike Emotet_f593ee31	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is f593ee319ae20d58340113b6d1a1e23c.
Strike Emotet_f81c62a7	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is f81c62a7bed4734b55bdb6d123449022.
Strike Emotet_f889195d	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is f889195d7fb07a26bb6597e61d659257.
Strike Emotet_f9c9f904	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is f9c9f904c00f64da4b188e5f3677097d.
Strike Emotet_fb3a1577	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is fb3a157718a1851fe9fccde52c5b7e11.
Strike Emotet_fc153f23	This strike sends a malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The MD5 hash of this Emotet sample is fc153f23c7f5c1d226313335dd7904eb.
Strike Emotet_fdb16564	This strike sends a polymorphic malware sample known as Emotet. Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Emotet sample is fdb16564b8d78cc7b97715394e958c64.
Strike ExelaStealer PDF executable_54293289	This strike sends a malware sample known as ExelaStealer PDF executable. ExelaStealer is a sophisticated and elusive Python-based malware. The malware primarily targets Discord users by modifying the Windows Discord client to steal sensitive information, including login credentials, personal data, and financial information, as well as session details from different online apps, social media services, and gaming platforms. This sample is the executable that launches the pdf viewer. The MD5 hash of this ExelaStealer PDF executable sample is 5429328937ed51076df9f8c4e5edc93a.

<b>Name</b>	<b>Description</b>
Strike ExelaStealer PDF executable_a774e196	This strike sends a malware sample known as ExelaStealer PDF executable. ExelaStealer is a sophisticated and elusive Python-based malware. The malware primarily targets Discord users by modifying the Windows Discord client to steal sensitive information, including login credentials, personal data, and financial information, as well as session details from different online apps, social media services, and gaming platforms. This sample is the executable that launches the pdf viewer. The MD5 hash of this ExelaStealer PDF executable sample is a774e1965dea429e097e4a3e1bef0943.
Strike ExelaStealer Runtime Broker_5c7805f8	This strike sends a malware sample known as ExelaStealer Runtime Broker. ExelaStealer is a sophisticated and elusive Python-based malware. The malware primarily targets Discord users by modifying the Windows Discord client to steal sensitive information, including login credentials, personal data, and financial information, as well as session details from different online apps, social media services, and gaming platforms. This sample is an executable. The MD5 hash of this ExelaStealer Runtime Broker sample is 5c7805f87a6e396231a360a4f350378f.
Strike ExelaStealer Runtime Broker_8b594b44	This strike sends a malware sample known as ExelaStealer Runtime Broker. ExelaStealer is a sophisticated and elusive Python-based malware. The malware primarily targets Discord users by modifying the Windows Discord client to steal sensitive information, including login credentials, personal data, and financial information, as well as session details from different online apps, social media services, and gaming platforms. This sample is an executable. The MD5 hash of this ExelaStealer Runtime Broker sample is 8b594b44addb55ebac34806dd0935181.
Strike Exorcist_0d256ab0	This strike sends a malware sample known as Exorcist. Exorcist is a new ransomware as a service that is distributed through Pastebin embedded in a Powershell script that loads itself directly in memory. The MD5 hash of this Exorcist sample is 0d256ab0a8b8b7a3b3d4aaf566189ca6.
Strike Exorcist_4908a364	This strike sends a polymorphic malware sample known as Exorcist. Exorcist is a new ransomware as a service that is distributed through Pastebin embedded in a Powershell script that loads itself directly in memory.The binary has the debug flag removed in the PE file format. The MD5 hash of this Exorcist sample is 4908a364b1d9467f2c9c3fcecccba202.
Strike Exorcist_55e43a8a	This strike sends a polymorphic malware sample known as Exorcist. Exorcist is a new ransomware as a service that is distributed through Pastebin embedded in a Powershell script that loads itself directly in memory.The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Exorcist sample is 55e43a8a489e4c9756a6375a15b2f102.
Strike Exorcist_5a63e7d3	This strike sends a malware sample known as Exorcist. Exorcist is a new ransomware as a service that is distributed through Pastebin embedded in a Powershell script that loads itself directly in memory. The MD5 hash of this Exorcist sample is 5a63e7d371dd69c5625f5b48da426c14.
Strike Exorcist_79385ed9	This strike sends a malware sample known as Exorcist. Exorcist is a new ransomware as a service that is distributed through Pastebin embedded in a Powershell script that loads itself directly in memory. The MD5 hash of this Exorcist sample is 79385ed97732aee0036e67824de18e28.

<b>Name</b>	<b>Description</b>
Strike Exorcist_7e415d5a	This strike sends a malware sample known as Exorcist. Exorcist is a new ransomware as a service that is distributed through Pastebin embedded in a Powershell script that loads itself directly in memory. The MD5 hash of this Exorcist sample is 7e415d5a1b1235491cb698eb14817d31.
Strike Exorcist_8cc13fea	This strike sends a malware sample known as Exorcist. Exorcist is a new ransomware as a service that is distributed through Pastebin embedded in a Powershell script that loads itself directly in memory. The MD5 hash of this Exorcist sample is 8cc13fea61cc0ba1382a779ee46726f0.
Strike Exorcist_cb3a1463	This strike sends a malware sample known as Exorcist. Exorcist is a new ransomware as a service that is distributed through Pastebin embedded in a Powershell script that loads itself directly in memory. The MD5 hash of this Exorcist sample is cb3a1463f4fd3e74b8f1ca5e73b81816.
Strike Exorcist_d4d32e75	This strike sends a malware sample known as Exorcist. Exorcist is a new ransomware as a service that is distributed through Pastebin embedded in a Powershell script that loads itself directly in memory. The MD5 hash of this Exorcist sample is d4d32e7583b3fd8363ded73c91ed3d08.
Strike Exorcist_e763b9a8	This strike sends a polymorphic malware sample known as Exorcist. Exorcist is a new ransomware as a service that is distributed through Pastebin embedded in a Powershell script that loads itself directly in memory. The binary has been packed using upx packer, with the default options. The MD5 hash of this Exorcist sample is e763b9a8460c2dc9a1229d0c8bf71ab4.
Strike Exorcist_f188cf26	This strike sends a malware sample known as Exorcist. Exorcist is a new ransomware as a service that is distributed through Pastebin embedded in a Powershell script that loads itself directly in memory. The MD5 hash of this Exorcist sample is f188cf267d209a0209a25bda4bb75b86.
Strike Exorcist_f4009abe	This strike sends a malware sample known as Exorcist. Exorcist is a new ransomware as a service that is distributed through Pastebin embedded in a Powershell script that loads itself directly in memory. The MD5 hash of this Exorcist sample is f4009abe9f41da41e48340c96e29d62c.
Strike Exorcist_fa4c4ac8	This strike sends a malware sample known as Exorcist. Exorcist is a new ransomware as a service that is distributed through Pastebin embedded in a Powershell script that loads itself directly in memory. The MD5 hash of this Exorcist sample is fa4c4ac8b9c1b14951ae8add855f34e8.
Strike Expilo_006d69c5	This strike sends a malware sample known as Expilo. Expilo or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expilo sample is 006d69c55af445e249fa154e4f31e55a.
Strike Expilo_0155baf3	This strike sends a malware sample known as Expilo. Expilo also known as Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expilo sample is 0155baf3b793202061b0c43ca7c9cec2.

<b>Name</b>	<b>Description</b>
Strike Expiro_01eeb5c6	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 01eeb5c6a9382fe8bc0691971dcda6da.
Strike Expiro_02191a87	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 02191a875603620180d8e1ce5766176a.
Strike Expiro_0413d149	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 0413d149c8f13c37c59b4045d19e104b.
Strike Expiro_04e0b84b	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 04e0b84b8474dcefbc68b7782cf61fa3.
Strike Expiro_0e9dcdba	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 0e9dcdba66ee4d9753292f4112a4537b.
Strike Expiro_128f886f	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 128f886f38ce715bfbe08fedd12e0173.
Strike Expiro_17661350	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 1766135009a50699dd4746150e78d14d.
Strike Expiro_1abac5c7	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 1abac5c78347e86a9b1969037cad5e5e.
Strike Expiro_1f0e8f82	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 1f0e8f826901b1a0ee03d9f73f48609c.
Strike Expiro_21c224a0	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 21c224a0e05ba44213104e8f4ae66132.
Strike Expiro_250f4f91	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 250f4f917a22885c0ee7fe96f6743c7a.
Strike Expiro_2f1f1c29	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 2f1f1c29323c486eb5e256a8c1f16050.

<b>Name</b>	<b>Description</b>
Strike Expiro_30f54fca	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 30f54fcac7e14e7cb1cc22bcca545a60.
Strike Expiro_31b46dee	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 31b46dee8917e8d73638bc3cca7c64ce.
Strike Expiro_34c50d3b	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 34c50d3baf3bfdc586c0a5127f2d1199.
Strike Expiro_35e46887	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 35e46887a497633076821bc083f29dff.
Strike Expiro_396b70ca	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 396b70ca9866d732f8a3912d30743237.
Strike Expiro_3daeaa3b8	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 3daeaa3b8bbb4ead9495ee4aff49b3a83.
Strike Expiro_3f328551	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 3f328551144c693d7e93d15929b61f73.
Strike Expiro_3f71b02f	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 3f71b02ff093f424563ddce686a2b6f4.
Strike Expiro_40c756f6	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 40c756f6a8b4c1944540fa90b0658bcf.
Strike Expiro_42647244	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 42647244735a032629d454fb2c70326e.
Strike Expiro_43d02938	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 43d0293877c77a8d6686fefef31c48e2a.
Strike Expiro_4458b006	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 4458b00653b951bc82cb9e7319a287fd.

<b>Name</b>	<b>Description</b>
Strike Expiro_4793202c	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 4793202c28081a9541b23c2e70b720c2.
Strike Expiro_4f42c310	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 4f42c3100de4b453ab5f13a1b66792b5.
Strike Expiro_506c9e8d	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 506c9e8dba60419f3956cd6f2860b60a.
Strike Expiro_5146796f	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 5146796f105b5a619b59e6ded6b53fb3.
Strike Expiro_53380954	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 533809544298d123d82695dae9c80451.
Strike Expiro_53489e71	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 53489e7181fa238fb2161a26487cbd56.
Strike Expiro_550cab38	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 550cab38c32073db8b332701584439fe.
Strike Expiro_56edfa30	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 56edfa303cf02984450540bb6d5b664.
Strike Expiro_62474ba0	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 62474ba004c093fb91c6a58b6d5a7c35.
Strike Expiro_70ce59f2	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 70ce59f24d63d6cf7c435ad54e1f39be.
Strike Expiro_7361a96f	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 7361a96fa8f72eb7d6b27ce60d10daca.
Strike Expiro_778eaf8a	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 778eaf8acb4055693ac74c98c073a3a6.

<b>Name</b>	<b>Description</b>
Strike Expiro_7e379a9a	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 7e379a9a3a6a2bc52ac50157b6239c95.
Strike Expiro_8080128d	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 8080128da1c704c1a3ef2f1cd8f7bc2c.
Strike Expiro_84a0b33b	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 84a0b33bd84b06b696919b48c0a4498b.
Strike Expiro_86174a83	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 86174a83ca172ce4d48cc347c92f780b.
Strike Expiro_8bb30113	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 8bb301137c9cf0781df8dcfd295d904dc.
Strike Expiro_92ee6e8d	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 92ee6e8d9cf8083bf2089fbce77c66e.
Strike Expiro_93dd0e8c	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 93dd0e8c12fdb1d378825a5a290cb39b.
Strike Expiro_940ad1e5	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is 940ad1e5108f90c6b7b59f07d4bdf364.
Strike Expiro_a17459cc	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is a17459ccfe7c29ee3860a86ce3841490.
Strike Expiro_a1a42c4c	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is a1a42c4c4f8e99f18e9dac5e0195a117.
Strike Expiro_a2f7ae1d	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is a2f7ae1ddd9611233e0cd0b29202e653.
Strike Expiro_a303b393	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is a303b3938a88af0faf21b8877085d7b5.

<b>Name</b>	<b>Description</b>
Strike Expiro_a5106972	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is a51069723865a6aba2a58439c373801d.
Strike Expiro_a519ccd4	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is a519ccd41237377fd6ff189fc34aa4a2.
Strike Expiro_a96008e0	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is a96008e0c13b46ba555464e1b9fc681f.
Strike Expiro_a9929ed0	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is a9929ed0a4b86f22d6773ba7f3a309f2.
Strike Expiro_ab58a757	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is ab58a757aa734d1ee7beba9262ea851f.
Strike Expiro_ae1693e9	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is ae1693e916245a7cbe94536db6c2dfb9.
Strike Expiro_af6d133b	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is af6d133b00f8311005ff302f03e2f93f.
Strike Expiro_b08ad0e8	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is b08ad0e8469c891ff4f71ba623e18d01.
Strike Expiro_b167581f	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is b167581fcb856d403e0c2163ced4a080.
Strike Expiro_b45603d9	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is b45603d9ea29859e52e80cf2d5169ce7.
Strike Expiro_b6200879	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is b62008793dce122676720498b66b9a14.
Strike Expiro_b91e0df6	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is b91e0df66b0a012a90db1ebfcfaa28b7.

<b>Name</b>	<b>Description</b>
Strike Expiro_b947b154	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is b947b15406b13614d0f8cdeec8564d05.
Strike Expiro_c30aa578	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is c30aa5781932f3368e1f53d285433873.
Strike Expiro_c3a4c6fc	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is c3a4c6fc3924bea9ff0af427a1595380.
Strike Expiro_c3e02b8e	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is c3e02b8ec2aee25f4ceac1773696b924.
Strike Expiro_c47b8c02	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is c47b8c02e838398bf9a3afc757fdb802.
Strike Expiro_c54812ff	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is c54812ffecccb9d42b6af9d85329fb10.
Strike Expiro_c5877275	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is c5877275ffbfa064142094638cb4dc9.
Strike Expiro_c6367980	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is c636798029addfe9cd1dfb144182ff2d.
Strike Expiro_c71fb079	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is c71fb07961cd7b69347f2cb2a6d8a30a.
Strike Expiro_c7a25967	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is c7a259674474b0eab3a37fab1b08f826.
Strike Expiro_ca458d5e	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is ca458d5e66b2b83b95a6af019fc7f298.
Strike Expiro_ca95f186	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is ca95f18632c18edea8580ffd5443bb57.

<b>Name</b>	<b>Description</b>
Strike Expiro_cb601c51	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is cb601c51cd742f846c50e3feddceb789.
Strike Expiro_ceb637aa	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is ceb637aa93f653ec7fd14dfec80ddec2.
Strike Expiro_cfec50d3	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is cfec50d3ddb50a9ebd752d069837ee2b.
Strike Expiro_d16af927	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is d16af927c910abff809b2a9f5372d855.
Strike Expiro_d3478d5b	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is d3478d5b7aa682818e253a6904e528b0.
Strike Expiro_d40dd121	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is d40dd121d3362943bf820a1749dfb7d3.
Strike Expiro_d82557b9	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is d82557b9bf7bcd552a37604c093a13cc.
Strike Expiro_d9a35ce3	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is d9a35ce3b7c6e201054527769d208dab.
Strike Expiro_e0522340	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is e0522340e4567dd1e9ec2f381826a019.
Strike Expiro_e16a3cdf	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is e16a3cdf66e2a3d2bbc0b512c79e5314.
Strike Expiro_e3f00ec8	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is e3f00ec88a61678f7aacdbd1d2a01bf4.
Strike Expiro_e4b2e04e	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is e4b2e04e617e3ccdb4bb5397fc9d04d5.

<b>Name</b>	<b>Description</b>
Strike Expiro_ee1389b2	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is ee1389b23c27eba03147d094e5da3355.
Strike Expiro_eee03c27	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is eee03c2746f5188eb4b2dc0ede35e9e5.
Strike Expiro_f654a322	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is f654a322a5da0d94ca89ae517c421d00.
Strike Expiro_f860c425	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is f860c425177e72337bbbb2ff4ca533ab.
Strike Expiro_f92e78f0	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is f92e78f03a38b86402273707777ad553.
Strike Expiro_fd75e90e	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is fd75e90e1c0fd610860085c1c642bf9c.
Strike Expiro_fdb1ca5f	This strike sends a malware sample known as Expiro. Expiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is fdb1ca5f6c337f9a501b7cafe3fb53cd.
Strike Expiro_ff06b123	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is ff06b1238c898d4450611bbeb1947ff3.
Strike Expiro_ff731130	This strike sends a malware sample known as Expiro. Expiro or Xpiro is a known file infector and information-stealer that hinders analysis with anti-debugging and anti-analysis tricks. The MD5 hash of this Expiro sample is ff7311302542ef3e9acd37302823b586.
Strike FROZEN#SHADOW JS_21c1d4d1	This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is 21c1d4d17e9305046d5e019d752aa33b.

<b>Name</b>	<b>Description</b>
Strike FROZEN#SHADOW JS_337504e8	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is 337504e854ded796695d2c1139517e43.</p>
Strike FROZEN#SHADOW JS_50c9e639	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is 50c9e63975fb626c2448aaaf193ca6aa.</p>
Strike FROZEN#SHADOW JS_53488dfc	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is 53488dfc8055b15c4f93c4ab4c55438c.</p>
Strike FROZEN#SHADOW JS_64e9b99d	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is 64e9b99d80a268eaaf1a8569802e7f70.</p>
Strike FROZEN#SHADOW JS_778d6626	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is 778d6626d730e9e35ec44050762b5845.</p>

<b>Name</b>	<b>Description</b>
Strike FROZEN#SHADOW JS_7d01cd13	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is 7d01cd13b456f87bf9e38c2cf5d30e16.</p>
Strike FROZEN#SHADOW JS_8be654aa	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is 8be654aa610119b38f3dde77419c3b82.</p>
Strike FROZEN#SHADOW JS_8c638dfd	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is 8c638dfdafd802371a6a1b068bdbea38.</p>
Strike FROZEN#SHADOW JS_9419f4e9	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is 9419f4e9d33b9e32b4fa1cb6e6028814.</p>
Strike FROZEN#SHADOW JS_9533cb63	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is 9533cb63facc2fcb4f6cfacb9e80075d.</p>

<b>Name</b>	<b>Description</b>
Strike FROZEN#SHADOW JS_ab63f751	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is ab63f751a6ce5758eb76c52f20322b06.</p>
Strike FROZEN#SHADOW JS_ce919274	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is ce919274cfb97ff411864b259091566f.</p>
Strike FROZEN#SHADOW JS_d174e68f	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is d174e68fe3458262e53dee5036eeb15e.</p>
Strike FROZEN#SHADOW JS_ecd4035e	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is ecd4035ecfb72e6883882abf14a9d84e.</p>
Strike FROZEN#SHADOW JS_efbe4a17	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is efbe4a17de6c0a8b251106225bf5f61f.</p>

<b>Name</b>	<b>Description</b>
Strike FROZEN#SHADOW JS_efc182e6	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is efc182e6f46d21d26f1132a72500620e.</p>
Strike FROZEN#SHADOW JS_f08acf04	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is f08acf0425732b3e9b72fee7daa4719a.</p>
Strike FROZEN#SHADOW JS_f85f33e5	<p>This strike sends a malware sample known as FROZEN#SHADOW JS. This malware is part of the FROZEN#SHADOW malware campaign. The campaign begins with a phishing email that redirects to a site to download a malicious obfuscated javascript file. This malware sample is that file. Once manually executed, it attempts to map a remote network drive to execute a .msi package. This package will then download and run the SSLoad malware payload. From here persistence is established on the victim machine and remote C2 communication is established which enables a host of options for the attacker including downloading and running Cobalt Strike. The MD5 hash of this FROZEN#SHADOW JS sample is f85f33e5ce5264618850cc4b9d79fda9.</p>
Strike Fakecalls-BankingTrojan_703b22fce	<p>This strike sends an Android banking trojan malware called Fakecalls. The particular sample was signed using a legitimate signing key same as that of reputable IT services Korean company app. It's a packed malware which includes a file introduction.html under the assets directory which is a second apk. This is then installed which has the typical behavior of a baking trojan. 'com.grn.nbz.ktvhe.xeubdv' is the package name of the malware sample. The MD5 hash of this trojan is 703b22fce432d2c681cebbc150394f1.</p>
Strike Fakecalls-BankingTrojan_821ed14c	<p>This strike sends an Android banking trojan polymorphic malware called Fakecalls. The particular sample was signed using a legitimate signing key same as that of reputable IT services Korean company app. It's a packed malware which includes a file introduction.html under the assets directory which is a second apk. This is then installed which has the typical behavior of a baking trojan. 'com.grn.nbz.ktvhe.xeubdv' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this trojan is 821ed14cd734237b802f520ae0cbc8c2.</p>

<b>Name</b>	<b>Description</b>
Strike Fakecalls-BankingTrojan_a0b47876	This strike sends an Android banking trojan polymorphic malware called Fakecalls. The particular sample was signed using a legitimate signing key same as that of reputable IT services Korean company app. It's a packed malware which includes a file introduction.html under the assets directory which is a second apk. This is then installed which has the typical behavior of a banking trojan. 'com.grn.nbz.ktvhe.xeubdv' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this trojan is a0b47876dff7d687cee88b0a3b899b21.
Strike FickerStealer_0e41b66c	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is 0e41b66cdedb024df77b4b6c884ebf4.
Strike FickerStealer_1162c25d	This strike sends a polymorphic malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this FickerStealer sample is 1162c25da0ef8cb976b4795ffc20da55.
Strike FickerStealer_149ed22a	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is 149ed22ad6665e56d2ae42609db48fc7.
Strike FickerStealer_14a1308a	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is 14a1308a84d9bff359cf560a1b370a92.
Strike FickerStealer_1b4d8385	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is 1b4d83858a7b6208b56b5dc2caddb6c5.
Strike FickerStealer_1c7e3ae0	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is 1c7e3ae095e7ae5de838b77e6ed32d19.
Strike FickerStealer_2b918de5	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is 2b918de59a843cebe559151f95aa07b9.
Strike FickerStealer_37269161	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is 3726916138308b8adb20433612bca5cc.
Strike FickerStealer_40044b19	This strike sends a polymorphic malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The Parent binary was packed using upx, hence this binary is the unpacked version generated using upx -d. The MD5 hash of this FickerStealer sample is 40044b19756860bd9543faf40e367e98.

<b>Name</b>	<b>Description</b>
Strike FickerStealer_48ef9ec3	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is 48ef9ec3c901229d96c3694c01b171b4.
Strike FickerStealer_63312fea	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is 63312fea232629e71c73b1515b65b110.
Strike FickerStealer_6751a44d	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is 6751a44d54a084b7b0d5750f8b89ae32.
Strike FickerStealer_6d5d6691	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is 6d5d6691a553839ad5493d99578173e9.
Strike FickerStealer_83e9401d	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is 83e9401d901b2aff0adaebc442b377e7.
Strike FickerStealer_960213df	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is 960213df917e78c3d354505a705f19e2.
Strike FickerStealer_9f664c6e	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is 9f664c6ee169b96b13de7c9468c126c6.
Strike FickerStealer_a48e3879	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is a48e38799e27137cae3ad69304b355c5.
Strike FickerStealer_a6cde2cc	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is a6cde2ccca89c27a450d55c0f4ce3273.
Strike FickerStealer_aff09cc7	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is aff09cc71b409bbbe3044a252d058f38.
Strike FickerStealer_b9c05fc9	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is b9c05fc9e7e83b917eeeb65d99ab1f7d.
Strike FickerStealer_bd3f88f3	This strike sends a polymorphic malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this FickerStealer sample is bd3f88f378327d538335b7adfd1c627b.

<b>Name</b>	<b>Description</b>
Strike FickerStealer_bdb1f644	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is bdb1f64404d82cf847550308cbad3e38.
Strike FickerStealer_c8341f08	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is c8341f0819c8cc287ff6ef841c532f35.
Strike FickerStealer_c8bd3efd	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is c8bd3efd6ab875e4f2770e636be24d08.
Strike FickerStealer_d12f2411	This strike sends a polymorphic malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The binary has the timestamp field updated in the PE file header. The MD5 hash of this FickerStealer sample is d12f241164758ff1e41a933a4fd5e270.
Strike FickerStealer_d220c5b8	This strike sends a polymorphic malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The binary has random bytes appended at the end of the file. The MD5 hash of this FickerStealer sample is d220c5b8a8ff304ded5745a82301e7f0.
Strike FickerStealer_d5557fd8	This strike sends a polymorphic malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The binary has the checksum removed in the PE file format. The MD5 hash of this FickerStealer sample is d5557fd865886af57958eeaf5897a042.
Strike FickerStealer_d5c015bb	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is d5c015bb5feec200f2848b31a143545.
Strike FickerStealer_deb3ef93	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is deb3ef9350a527f03d3c6b5f18b35c4e.
Strike FickerStealer_e38f3dc9	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is e38f3dc988a4549482997eff2c7ef784.
Strike FickerStealer_f8583d70	This strike sends a malware sample known as FickerStealer. FickerStealer is an infostealer that is written in Rust and can be purchased on Russian hacking forums. The MD5 hash of this FickerStealer sample is f8583d7073f13eb803f6aa5828bda061.
Strike Fickle Stealer_019f3bdb	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is 019f3bdbec3910e02de1888a4aff8409.

<b>Name</b>	<b>Description</b>
Strike Fickle Stealer_1313424c	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is 1313424ce8051962d4ce96826b0dc367.
Strike Fickle Stealer_390838a8	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is 390838a85591302af29356b7307d39f9.
Strike Fickle Stealer_57417e3a	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is 57417e3abbb4521f0b801e0c455b6450.
Strike Fickle Stealer_59b26d4e	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is 59b26d4eb00e9bcc57527d687958c1aa.
Strike Fickle Stealer_660acebe	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is 660acebe3c47ba2df649a2664ec67079.
Strike Fickle Stealer_67a83a0c	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is 67a83a0cc016579f1a11f177e888729d.
Strike Fickle Stealer_75a9090d	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is 75a9090db55edeb239562682e6d9836a.
Strike Fickle Stealer_75b9ef91	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is 75b9ef9142a78671d449c8d22ab6be14.

<b>Name</b>	<b>Description</b>
Strike Fickle Stealer_7a5cc3ab	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is 7a5cc3ab48c78ed9e9a52cbaa04c79bc.
Strike Fickle Stealer_8e7d3217	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is 8e7d32179baafa63e24465a0640c1cfb.
Strike Fickle Stealer_b563008b	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is b563008bdef8ce3d8598e97b2669170c.
Strike Fickle Stealer_bcebea94	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is bcebea947daeaa445418bc043d05d19fa.
Strike Fickle Stealer_d77bea7c	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is d77bea7c331aae01debc4b29a3f2d535.
Strike Fickle Stealer_d9b0f87a	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is d9b0f87a985c19f76efc91d975798cdf.
Strike Fickle Stealer_e6afbfea	This strike sends a malware sample known as Fickle Stealer. Fickle Stealer is an information stealer type of malware that exfiltrates sensitive data back to the attacker. The malware is written in Rust and is delivered via a VBA dropper, Link downloader or and executable downloader. It has many ways in which it evades security defenses and analysis. The MD5 hash of this Fickle Stealer sample is e6afbfea4258c7122cfdddc8dc6c4148.

<b>Name</b>	<b>Description</b>
Strike FinancialFraud_24704575	This strike sends a polymorphic malware sample known as Financial Fraud APK. The android malware disguises as a law enforcement app, deceiving victims into downloading it for a fake fraud investigation. Once installed, it blocks incoming calls and SMS messages, isolating victims from genuine alerts about financial fraud. By blocking calls and SMS, the app isolates victims, preventing legitimate alerts about fraud. The app further gains permissions to make calls and receive SMS messages, enabling control over communications. 'com.lfedajfl' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 247045753ccbb8cccd6a567d00641858b.
Strike FinancialFraud_7ca7a7f0	This strike sends a polymorphic malware sample known as Financial Fraud APK. The android malware disguises as a law enforcement app, deceiving victims into downloading it for a fake fraud investigation. Once installed, it blocks incoming calls and SMS messages, isolating victims from genuine alerts about financial fraud. By blocking calls and SMS, the app isolates victims, preventing legitimate alerts about fraud. The app further gains permissions to make calls and receive SMS messages, enabling control over communications. 'com.lfeffcis' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 7ca7a7f09975efe067e0794a5f485a03.
Strike FinancialFraud_82bc24c2	This strike sends a polymorphic malware sample known as Financial Fraud APK. The android malware disguises as a law enforcement app, deceiving victims into downloading it for a fake fraud investigation. Once installed, it blocks incoming calls and SMS messages, isolating victims from genuine alerts about financial fraud. By blocking calls and SMS, the app isolates victims, preventing legitimate alerts about fraud. The app further gains permissions to make calls and receive SMS messages, enabling control over communications. 'com.lfeffcis' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 82bc24c20680cdc16d0187ff7f69f605.
Strike FinancialFraud_8de830d3	This strike sends a malware sample known as Financial Fraud APK. The android malware disguises as a law enforcement app, deceiving victims into downloading it for a fake fraud investigation. Once installed, it blocks incoming calls and SMS messages, isolating victims from genuine alerts about financial fraud. By blocking calls and SMS, the app isolates victims, preventing legitimate alerts about fraud. The app further gains permissions to make calls and receive SMS messages, enabling control over communications. 'com.lfedajfl' is the package name of the malware sample. The MD5 hash of this malware sample is 8de830d3c621310cffa4d1197708626e.
Strike FinancialFraud_9470c327	This strike sends a malware sample known as Financial Fraud APK. The android malware disguises as a law enforcement app, deceiving victims into downloading it for a fake fraud investigation. Once installed, it blocks incoming calls and SMS messages, isolating victims from genuine alerts about financial fraud. By blocking calls and SMS, the app isolates victims, preventing legitimate alerts about fraud. The app further gains permissions to make calls and receive SMS messages, enabling control over communications. 'com.lfeffcis' is the package name of the malware sample. The MD5 hash of this malware sample is 9470c327fd545f58f090902f6f3001ed.

Name	Description
Strike FinancialFraud_bb444c16	This strike sends a polymorphic malware sample known as Financial Fraud APK. The android malware disguises as a law enforcement app, deceiving victims into downloading it for a fake fraud investigation. Once installed, it blocks incoming calls and SMS messages, isolating victims from genuine alerts about financial fraud. By blocking calls and SMS, the app isolates victims, preventing legitimate alerts about fraud. The app further gains permissions to make calls and receive SMS messages, enabling control over communications. 'com.lfedajfl' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is bb444c16d2c9dde377c855719e917582.
Strike Flodrix_0283e184	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is 0283e1842be85af8535b2c5489db75e1.
Strike Flodrix_112c3b26	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is 112c3b263a00ed8a3332b29a1b9da10e.
Strike Flodrix_271576e1	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is 271576e1886df2ea54fab470fba2fcc.
Strike Flodrix_295a83c4	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is 295a83c4d643f3f89ca87b45fd888a2f.

<b>Name</b>	<b>Description</b>
Strike Flodrix_34fe0e8a	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is 34fe0e8a3270379ce8696a856b501afe.
Strike Flodrix_3970432b	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is 3970432b39416722f1abdfb1e249b534.
Strike Flodrix_39b1f49b	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is 39b1f49ba958abaea54aa219c365270a.
Strike Flodrix_55d449a1	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is 55d449a1050aef47e52731bfd4339de5.
Strike Flodrix_70cc5f0a	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is 70cc5f0a17d7806eedc3d67774a9bfc6.

<b>Name</b>	<b>Description</b>
Strike Flodrix_77fa8103	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is 77fa81033d8cd8065870d13453fc5409.
Strike Flodrix_94315351	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is 943153516f578b5622a72d09aadc1c67.
Strike Flodrix_a6e71445	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is a6e71445d800c61040176e19cf3c54bb.
Strike Flodrix_bef8fc7f	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is bef8fc7f880e03f48e0efba57f1a3374.
Strike Flodrix_d629b5f5	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is d629b5f5a0971a1ef2262f6197f76466.

<b>Name</b>	<b>Description</b>
Strike Flodrix_da622893	This strike sends a malware sample known as Flodrix. This strike sends a malware sample known as Flodrix. Flodrix is a Linux-based botnet malware linked to the LeetHozer family. It is delivered through exploitation of CVE-2025-3248 in vulnerable Langflow servers. Once deployed, Flodrix establishes C2 communication and launches multi-vector DDoS attacks such as tcpraw, udpplain, and tcplegit. The malware employs evasion capabilities like process deception, artifact cleanup, and conditional self-deletion, while supporting cross-architecture payloads via versatile downloader scripts. The MD5 hash of this Flodrix sample is da62289386b20d8691ec5115be1cb368.
Strike FluBot_3a0db08d	This strike sends a malware sample known as FluBot. FluBot is a mobile Android malware that is part of a SMS campaign that spoofs different logistics companies like Fedex and DHL by giving the user a notification to install the application in order to locate a package. Once installed the application clones realistic logistic web sites to send the user credentials back to a C2 server. The malware exfiltrates other user data like contacts list in order to spam contacts. The MD5 hash of this FluBot sample is 3a0db08d86d3d57edea7d52843f32761.
Strike FluBot_4125019b	This strike sends a malware sample known as FluBot. FluBot is a mobile Android malware that is part of a SMS campaign that spoofs different logistics companies like Fedex and DHL by giving the user a notification to install the application in order to locate a package. Once installed the application clones realistic logistic web sites to send the user credentials back to a C2 server. The malware exfiltrates other user data like contacts list in order to spam contacts. The MD5 hash of this FluBot sample is 4125019bb3370f1f659f448a5727357c.
Strike FluBot_6d879ac0	This strike sends a malware sample known as FluBot. FluBot is a mobile Android malware that is part of a SMS campaign that spoofs different logistics companies like Fedex and DHL by giving the user a notification to install the application in order to locate a package. Once installed the application clones realistic logistic web sites to send the user credentials back to a C2 server. The malware exfiltrates other user data like contacts list in order to spam contacts. The MD5 hash of this FluBot sample is 6d879ac01f7a26d62b38d9473626a328.
Strike FluBot_749510b3	This strike sends a malware sample known as FluBot. FluBot is a mobile Android malware that is part of a SMS campaign that spoofs different logistics companies like Fedex and DHL by giving the user a notification to install the application in order to locate a package. Once installed the application clones realistic logistic web sites to send the user credentials back to a C2 server. The malware exfiltrates other user data like contacts list in order to spam contacts. The MD5 hash of this FluBot sample is 749510b3010a45fea2d2763476e17511.
Strike FluBot_7b4fd668	This strike sends a malware sample known as FluBot. FluBot is a mobile Android malware that is part of a SMS campaign that spoofs different logistics companies like Fedex and DHL by giving the user a notification to install the application in order to locate a package. Once installed the application clones realistic logistic web sites to send the user credentials back to a C2 server. The malware exfiltrates other user data like contacts list in order to spam contacts. The MD5 hash of this FluBot sample is 7b4fd668a684e9bb6d09bcf2ebadfd2.

<b>Name</b>	<b>Description</b>
Strike FluBot_891d5d2c	This strike sends a malware sample known as FluBot. FluBot is a mobile Android malware that is part of a SMS campaign that spoofs different logistics companies like Fedex and DHL by giving the user a notification to install the application in order to locate a package. Once installed the application clones realistic logistic web sites to send the user credentials back to a C2 server. The malware exfiltrates other user data like contacts list in order to spam contacts. The MD5 hash of this FluBot sample is 891d5d2c397e9ad5fed5685f78657d4b.
Strike FluBot_8b6c4905	This strike sends a malware sample known as FluBot. FluBot is a mobile Android malware that is part of a SMS campaign that spoofs different logistics companies like Fedex and DHL by giving the user a notification to install the application in order to locate a package. Once installed the application clones realistic logistic web sites to send the user credentials back to a C2 server. The malware exfiltrates other user data like contacts list in order to spam contacts. The MD5 hash of this FluBot sample is 8b6c4905f8f93af27e60b502621e03f6.
Strike FluBot_9ef4f52a	This strike sends a malware sample known as FluBot. FluBot is a mobile Android malware that is part of a SMS campaign that spoofs different logistics companies like Fedex and DHL by giving the user a notification to install the application in order to locate a package. Once installed the application clones realistic logistic web sites to send the user credentials back to a C2 server. The malware exfiltrates other user data like contacts list in order to spam contacts. The MD5 hash of this FluBot sample is 9ef4f52a6ed459eab6311a4a886ec1ea.
Strike FluBot_a45dc99d	This strike sends a malware sample known as FluBot. FluBot is a mobile Android malware that is part of a SMS campaign that spoofs different logistics companies like Fedex and DHL by giving the user a notification to install the application in order to locate a package. Once installed the application clones realistic logistic web sites to send the user credentials back to a C2 server. The malware exfiltrates other user data like contacts list in order to spam contacts. The MD5 hash of this FluBot sample is a45dc99d0d146524d608691f86d00d63.
Strike FluBot_c10d38a6	This strike sends a malware sample known as FluBot. FluBot is a mobile Android malware that is part of a SMS campaign that spoofs different logistics companies like Fedex and DHL by giving the user a notification to install the application in order to locate a package. Once installed the application clones realistic logistic web sites to send the user credentials back to a C2 server. The malware exfiltrates other user data like contacts list in order to spam contacts. The MD5 hash of this FluBot sample is c10d38a63e776e5940d281bddbb497d4.
Strike ForestTiger_9c860ec3	This strike sends a malware sample known as ForestTiger. ForestTiger is a backdoor payload that has been identified in the Diamond Sleet North Korean cyber attacks against TeamCity servers. After it is downloaded via powershell and executed, it decrypts the C2 configuration file, creates a scheduled task and dumps credentials. The MD5 hash of this ForestTiger sample is 9c860ec31e77c73805372299e36e4473.

<b>Name</b>	<b>Description</b>
Strike ForestTiger_fff1e249	This strike sends a malware sample known as ForestTiger. ForestTiger is a backdoor payload that has been identified in the Diamond Sleet North Korean cyber attacks against TeamCity servers. After it is downloaded via powershell and executed, it decrypts the C2 configuration file, creates a scheduled task and dumps credentials. The MD5 hash of this ForestTiger sample is fff1e24971d48bb8884dee321f93c0f5.
Strike Formbook_01808133	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 01808133083391521ebac24a87e78dd7.
Strike Formbook_04bdc16c	This strike sends a polymorphic malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Formbook sample is 04bdc16ce9fac909ff5f70444c45c160.
Strike Formbook_0912eed1	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 0912eed158ab6a7f1c0ee050ae08b4dc.
Strike Formbook_09832f42	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 09832f42326e63a715e22cc8c54b0600.
Strike Formbook_0bff8d0d	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 0bff8d0d01a06645782ecea620ac5fc.
Strike Formbook_0c8e247e	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 0c8e247e7049fe06bfcc96aa48de0f.
Strike Formbook_0d6b09e8	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 0d6b09e8ded8569b94bc181419a4b3db.
Strike Formbook_137f641f	This strike sends a polymorphic malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The binary file has one more imports added in the import table. The MD5 hash of this Formbook sample is 137f641fab0889a53ce35c1e945ff143.
Strike Formbook_1841788c	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 1841788c0f23da54626ce38767caea99.

<b>Name</b>	<b>Description</b>
Strike Formbook_1ee76569	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 1ee765692e594d7a016424e6515bfe1f.
Strike Formbook_27765727	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 27765727c5049dc8be15211d83f12326.
Strike Formbook_2983786e	This strike sends a polymorphic malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Formbook sample is 2983786eb8a2877879dd7bbb2bafc8ae.
Strike Formbook_2a414be7	This strike sends a polymorphic malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The binary has the checksum removed in the PE file format. The MD5 hash of this Formbook sample is 2a414be7c6dea6d4d1bfd77c3e9c9b25.
Strike Formbook_2ba0a2a0	This strike sends a polymorphic malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The binary has random bytes appended at the end of the file. The MD5 hash of this Formbook sample is 2ba0a2a0b3fb79d8a72b992860e00c10.
Strike Formbook_329f7e4e	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 329f7e4e00314e9cb074d15b2347df16.
Strike Formbook_376dd288	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 376dd2886e40bf04651900326d436943.
Strike Formbook_3887644a	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 3887644a8b40a31b9916c390acff825c.
Strike Formbook_3915ee59	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 3915ee5917342673cd8edf72819784e6.
Strike Formbook_395b256d	This strike sends a polymorphic malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Formbook sample is 395b256db9fe92555d8ffbcd63331d4.

<b>Name</b>	<b>Description</b>
Strike Formbook_3e1ffccb	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 3e1ffccb84319f3691ca70978d0133da.
Strike Formbook_3e413c65	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 3e413c65154648fe22b554398986ae4d.
Strike Formbook_4131d35e	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 4131d35ec6a865907eddc8faa8cce33.
Strike Formbook_42e783c3	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 42e783c3fce437f1ea7eaa89c45b31e6.
Strike Formbook_440e6d38	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 440e6d387a6a202fb695171cdd90e9f0.
Strike Formbook_44bf8f92	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 44bf8f92e9f2f06894bc8b897202baf4.
Strike Formbook_457f3c74	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 457f3c7400382ec8ebe7885d1c666aeb.
Strike Formbook_495b6897	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 495b689701ab45f119a9ec53810e0e09.
Strike Formbook_49fa2aec	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 49fa2aecca84c2cccd83b20297143646.
Strike Formbook_4b5e6a79	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 4b5e6a79736d1e17a28120d6002de95c.
Strike Formbook_4c2e538c	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 4c2e538cb6b68a7d8c36cdfcd1a845ef.

<b>Name</b>	<b>Description</b>
Strike Formbook_4d3c739b	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 4d3c739bab68b3eea8cd032aef303525.
Strike Formbook_4d4663b4	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 4d4663b468bae17f8bd9ddd835293d50.
Strike Formbook_4ea9dea5	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 4ea9dea514d89ea4bf1a9231797f228e.
Strike Formbook_4f631559	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 4f6315593f81cee989d2d2c376869e5a.
Strike Formbook_50ca25d3	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 50ca25d3b67f76c1a39fd08262d759a1.
Strike Formbook_51a4e7af	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 51a4e7aff8e4f4a498749fa9cbdc52fe.
Strike Formbook_51d38940	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 51d38940d12472a0c3eb710fa8aa48e2.
Strike Formbook_530ed7ba	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 530ed7ba1cd9425cc5bf2a8be3727305.
Strike Formbook_54497e2f	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 54497e2f3ef3331eba62e146a4bbbcf4.
Strike Formbook_546b3cc7	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 546b3cc7640a0c3105f6674fd9e2debf.
Strike Formbook_54cfac04	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 54cfac04999f1abb22af7c20823fb2a1.

<b>Name</b>	<b>Description</b>
Strike Formbook_564ef895	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 564ef895bb45e19d54814fe65bf9efa4.
Strike Formbook_5742fec2	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 5742fec23905873e891ea7329acd3970.
Strike Formbook_5f2454c9	This strike sends a polymorphic malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Formbook sample is 5f2454c9c919b31b70366d2c34c14b4a.
Strike Formbook_6127f5d1	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 6127f5d1a39a07a6a33155f9181bd5c4.
Strike Formbook_659a7625	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 659a76255f7333ec04875008570a8a40.
Strike Formbook_74556c50	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 74556c50f37bc613e26d6c69383ba6c9.
Strike Formbook_783a8f3a	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 783a8f3a3d9f1f92e310775bc1bc3bf3.
Strike Formbook_79071d4b	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 79071d4b37fd17e5e11aa6519894631f.
Strike Formbook_7c863257	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 7c863257a55bf029ffa58f2ed25ae22c.
Strike Formbook_7e04266f	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 7e04266f63806aedf5b5643de2672ee8.
Strike Formbook_7ecee2ab	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 7ecee2ab9f46ab359d0978df98ac4faf.

<b>Name</b>	<b>Description</b>
Strike Formbook_800b669f	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 800b669f5722ce9be29327319cd98f03.
Strike Formbook_857e3a6e	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 857e3a6ecbeada63ae04fc1471abffcd.
Strike Formbook_88bf6373	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 88bf6373c1b7134bccd4b734f81f67be.
Strike Formbook_8a8fa678	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 8a8fa678e6d18beffd6edf5ab7c8f87a.
Strike Formbook_8ec040b5	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 8ec040b599ca27c33a5503834d0b666f.
Strike Formbook_8f905d0c	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 8f905d0c1831985db19e53d2b442fdb4.
Strike Formbook_8fd89c48	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 8fd89c48fdacb3ba7a8cb003917c24c3.
Strike Formbook_905d5725	This strike sends a polymorphic malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The binary has the checksum removed in the PE file format. The MD5 hash of this Formbook sample is 905d5725cd20bea4c5024f456c07f59a.
Strike Formbook_970841bd	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 970841bdc961619f7665e347ef1806b1.
Strike Formbook_979aed7e	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is 979aed7e10bcfd3c9ddf7742fc3848f0.

<b>Name</b>	<b>Description</b>
Strike Formbook_a08ca774	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is a08ca774bbbc6f7f42aa7b4fede272b0.
Strike Formbook_a2a964f2	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is a2a964f29b250bc0a0f02dc27da66af7.
Strike Formbook_a2b2a436	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is a2b2a436dbc3040c0689bb915d8d03ac.
Strike Formbook_a6e2e7b8	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is a6e2e7b8432f69b33934a8cdde050c14.
Strike Formbook_a815304b	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is a815304b1a9d216a410082490224e4d8.
Strike Formbook_a8cea309	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is a8cea309992bd4d8ba810a134c6e42f9.
Strike Formbook_b002ce46	This strike sends a polymorphic malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Formbook sample is b002ce46b1e46169da575d284a9b9656.
Strike Formbook_b0de6a61	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is b0de6a61550374c5e342fd91ee21533.
Strike Formbook_b143497e	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is b143497e7326cd491c695b556640192b.
Strike Formbook_b320feef	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is b320feefe49c10a68c1dd8fc5d9dd5b6.
Strike Formbook_b5035713	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is b50357138009c1963250582b787bd78a.

<b>Name</b>	<b>Description</b>
Strike Formbook_b93a2f5e	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is b93a2f5eb85ed74a4a3483fe63f2efe2.
Strike Formbook_ba6b36b0	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is ba6b36b03f1864c1adb63a87ae843ee3.
Strike Formbook_bb9c642b	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is bb9c642b4346962dd8e0ffd60c227862.
Strike Formbook_bea316e0	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is bea316e056c7db49d33b4fbfdc052504.
Strike Formbook_c16254c0	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is c16254c097c56d8fd2ac182457b4e9d4.
Strike Formbook_c1930047	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is c1930047f21a89ddfba5a2e2db2d5485.
Strike Formbook_c3a2687b	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is c3a2687bee4d3a1711b6d0dd63777df1.
Strike Formbook_c7427f66	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is c7427f66130867e74aa2bb018117d5fb.
Strike Formbook_cbb865bc	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is cbb865bcf8313c65329c275f024fe7a6.
Strike Formbook_d09e6818	This strike sends a polymorphic malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Formbook sample is d09e6818c698e74122c673c14082c603.

<b>Name</b>	<b>Description</b>
Strike Formbook_d16bb207	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is d16bb20744b2d89ed3bd10f146dec18b.
Strike Formbook_d1b9de2c	This strike sends a polymorphic malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The binary has the checksum removed in the PE file format. The MD5 hash of this Formbook sample is d1b9de2c6b6040b9ba71b1566dc8d76d.
Strike Formbook_d1ef4711	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is d1ef4711e6d940cfbd343767f94d5f4.
Strike Formbook_da8413de	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is da8413de8d3e993911acbc14f04a5881.
Strike Formbook_e06e23ac	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is e06e23accadab6d63e435ad52ca29f92.
Strike Formbook_e1884f7b	This strike sends a polymorphic malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The binary has random bytes appended at the end of the file. The MD5 hash of this Formbook sample is e1884f7ba2ea239be6cecbff1c5ba1b.
Strike Formbook_e429872a	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is e429872acbbb4ddd0510a6938256b435.
Strike Formbook_e8803f42	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is e8803f423d78f5000ba4e74e4ce20f30.
Strike Formbook_e890cec2	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is e890cec215217d4bb349ed6d944f018d.
Strike Formbook_ea291e84	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is ea291e8474afb136488146a924348693.
Strike Formbook_ed023da1	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is ed023da1556dcf73ce6657ae1642194a.

<b>Name</b>	<b>Description</b>
Strike Formbook_ed588185	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is ed588185aacf2a9ea91b31af93642256.
Strike Formbook_f049eeb6	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is f049eeb6a65e3730356fe9f64948fead.
Strike Formbook_f416d6cb	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is f416d6cb3fe1c8dcfe901640810c34da.
Strike Formbook_f5224cd8	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is f5224cd89a4c889a4dbff21a7386370a.
Strike Formbook_f8684b50	This strike sends a malware sample known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is f8684b50a83b7077ab75af9bc5913976.
Strike Formbook_fa710797	This strike sends a malware sample known as Formbook. This malicious sample is known as Formbook. Formbook is an information stealer that attempts to collect sensitive information from the target. The MD5 hash of this Formbook sample is fa7107970a5b56d0d2c4b5692dbd9d33.
Strike Frozenlake_2b025232	This strike sends a malware sample known as Frozenlake. Frozenlake aka APT28 is a spear phishing campaign exploiting a winRAR vulnerability (CVE-2023-38831) to deliver malware targeting energy infrastructure. The MD5 hash of this Frozenlake sample is 2b02523231105ff17ea07b0a7768f3fd.
Strike Frozenlake_9af76e61	This strike sends a malware sample known as Frozenlake. Frozenlake aka APT28 is a spear phishing campaign exploiting a winRAR vulnerability (CVE-2023-38831) to deliver malware targeting energy infrastructure. The MD5 hash of this Frozenlake sample is 9af76e61525fe6c89fe929ac5792ab62.
Strike Gamaredon LNK_00c48e42	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 00c48e429910f71e5057b65c5da8969a.
Strike Gamaredon LNK_0248e574	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 0248e574d4c81c09385db6fa80cab0e.

<b>Name</b>	<b>Description</b>
Strike Gamaredon LNK_0266e77c	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 0266e77c7123420098b9a05da08007e0.
Strike Gamaredon LNK_07cf4859	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 07cf485907f7fcf695367196e61936ff.
Strike Gamaredon LNK_0a1a5b43	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 0a1a5b431ac183e72e18ca88288e6759.
Strike Gamaredon LNK_0cbf38cf	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 0cbf38cf6874089b7958eb3327d8d4f3.
Strike Gamaredon LNK_0d08e2f8	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 0d08e2f8fee794e356d1a01b5bb38b87.
Strike Gamaredon LNK_0d26b815	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 0d26b815e67b5fee7289c0a83251163f.
Strike Gamaredon LNK_0db436da	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 0db436dafbe1b64eeb7caaefbe26ff05.
Strike Gamaredon LNK_1148abd5	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 1148abd57acdfb47206dcc990fd9333c.
Strike Gamaredon LNK_11fcebed	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 11fcebede652f2cda0cc7b0b1d351b51.
Strike Gamaredon LNK_149936e1	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 149936e1985b9318ad058472467aa229.

<b>Name</b>	<b>Description</b>
Strike Gamaredon LNK_1664d5f3	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 1664d5f3dc065840b88ee13b4b929e16.
Strike Gamaredon LNK_1dac3087	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 1dac308724b3195bb936ac80d7266ebe.
Strike Gamaredon LNK_1dd11223	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 1dd11223c483ef8f360e69b6c298a4be.
Strike Gamaredon LNK_200a34e4	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 200a34e46bda05e68191aea02d12ed9e.
Strike Gamaredon LNK_22a18dc4	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 22a18dc4988e6c1e59a1b3d54fc2016a.
Strike Gamaredon LNK_26767ece	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 26767ecebd6e9f2c0b7cda3ecfd90982.
Strike Gamaredon LNK_2c666d7b	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 2c666d7b2674a30c444f459041f0da30.
Strike Gamaredon LNK_2ef9d18e	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 2ef9d18e66a0e657c9f124cce0b38b5f.
Strike Gamaredon LNK_3067d11b	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 3067d11bca1acb7c99fd33035d66d96a.
Strike Gamaredon LNK_35963e2c	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 35963e2cb622326df9dbad92cb10c373.

<b>Name</b>	<b>Description</b>
Strike Gamaredon LNK_380fc5c6	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 380fc5c6fa55301e1feb1511b135448a.
Strike Gamaredon LNK_3dba2da9	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 3dba2da97e82193d646b059364016f5f.
Strike Gamaredon LNK_41592fa9	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 41592fa9dad0601a59eb316af0ac7627.
Strike Gamaredon LNK_41f6fc3e	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 41f6fc3ef347dc8b3b0b6740a7346714.
Strike Gamaredon LNK_48e47b1f	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 48e47b1ff522b549a2a331909faf54d3.
Strike Gamaredon LNK_4f3b3c5b	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 4f3b3c5b8b30f8540cadfeff796463a7.
Strike Gamaredon LNK_4fd8351f	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 4fd8351f8f1ca3902f7c901632771d58.
Strike Gamaredon LNK_5b139636	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 5b1396364c0c0d20ab3dc4767dc8e91.
Strike Gamaredon LNK_5ca29f15	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 5ca29f15a8b49081746a43235ee78db6.
Strike Gamaredon LNK_5eb312ac	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 5eb312acd225e757fec0b6fb6a1d0d12.

<b>Name</b>	<b>Description</b>
Strike Gamaredon LNK_5ef499a7	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 5ef499a770f5d5583d5d232ed2aaf66b.
Strike Gamaredon LNK_69792d7c	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 69792d7c8f23f9832331c4ef8c12bc12.
Strike Gamaredon LNK_76202703	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 76202703c97dce1360a0996ad7fba8a3.
Strike Gamaredon LNK_83c03dc8	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 83c03dc8c0ee23af38698a0c378b7acb.
Strike Gamaredon LNK_870d291e	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 870d291e7c77e6f588fcadb87da4f052.
Strike Gamaredon LNK_87619571	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 87619571a8b1b30c00b74b7c7f0649fe.
Strike Gamaredon LNK_8888e5bb	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 8888e5bb7ef8199d87253179b7269bfc.
Strike Gamaredon LNK_8a54378e	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 8a54378e0886fae831124c45af90b7dc.
Strike Gamaredon LNK_8b97b4d4	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 8b97b4d4905e9e01ac7c3f5d27ab5f28.
Strike Gamaredon LNK_905dc7c2	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 905dc7c24e3145943df6866e17e18d54.

<b>Name</b>	<b>Description</b>
Strike Gamaredon LNK_9b797330	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 9b79733073215925d05220873a3c7442.
Strike Gamaredon LNK_9bac38e9	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 9bac38e9d321017e1376f7928901f6cd.
Strike Gamaredon LNK_9bde92d2	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 9bde92d297d4e39fc88986346bf6ceb3.
Strike Gamaredon LNK_9d45119a	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 9d45119ab2f821a5fc5f87a28e579b5.
Strike Gamaredon LNK_9e1f6d2d	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is 9e1f6d2d25193f5d31c1ee8338b1a72c.
Strike Gamaredon LNK_ac3ede06	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is ac3ede06c848967bacb10bbb2709c38c.
Strike Gamaredon LNK_acff2d4f	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is acff2d4f5a0bc41a3d300ff751bc26b2.
Strike Gamaredon LNK_adef048a	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is adef048a1d39a8022a48dd6afe839358.
Strike Gamaredon LNK_b359682d	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is b359682d874fc19cf48c9e37c8fb996.
Strike Gamaredon LNK_b8a1d2e3	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is b8a1d2e3fb32be2559a3808cf50c6c7b.

<b>Name</b>	<b>Description</b>
Strike Gamaredon LNK_b9f6480d	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is b9f6480d05ba5fa910de8bec443d3e00.
Strike Gamaredon LNK_bd498131	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is bd498131945d5e2ff248835f82107eee.
Strike Gamaredon LNK_bd7464c3	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is bd7464c39668285e08d8501dbc0a85d0.
Strike Gamaredon LNK_bedef6c2	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is bedef6c253fc2b7b0dda41f234c518ee.
Strike Gamaredon LNK_c034427e	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is c034427e188e350640e82a5c958f9d5c.
Strike Gamaredon LNK_c50070ec	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is c50070ec82a2a961b536d0165b9842d1.
Strike Gamaredon LNK_cffb40e1	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is cffb40e13e3aa6761330090b42314c36.
Strike Gamaredon LNK_d30fa7cf	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is d30fa7cf31d3d4219223a97b59217bd3.
Strike Gamaredon LNK_d3652d3e	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is d3652d3e3af89f56f3422362f9f84651.
Strike Gamaredon LNK_d8aa4011	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is d8aa4011f6e62b9662e90f800d0212bc.

<b>Name</b>	<b>Description</b>
Strike Gamaredon LNK_dade5d04	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is dade5d04fc5853b76fde619d01b35d23.
Strike Gamaredon LNK_e3955358	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is e395535867ec62584c77a6668d4439ea.
Strike Gamaredon LNK_e68ab294	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is e68ab294b7de55fdaae8a3fae486d9b9.
Strike Gamaredon LNK_e79a1a46	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is e79a1a46c2a363bac3eae7a122be5746.
Strike Gamaredon LNK_ea7a9154	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is ea7a91548b1e3445a3aa300f9d58c4ee.
Strike Gamaredon LNK_eb237477	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is eb237477d0f7660b43d3e192e61a8e3d.
Strike Gamaredon LNK_ee092c14	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is ee092c1452997ffb29a4c9ab1888d6ca.
Strike Gamaredon LNK_f45b30a6	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is f45b30a6a34861e5c95d5a517b28f640.
Strike Gamaredon LNK_f7c1a41d	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is f7c1a41dae50556374a65a4b348d6801.
Strike Gamaredon LNK_f81e6239	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is f81e62397bdf3eb3d580a3287eadfbc1.

<b>Name</b>	<b>Description</b>
Strike Gamaredon LNK_f97902ff	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is f97902ff0d361801ca4756d692141ab2.
Strike Gamaredon LNK_f9c13294	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is f9c132945b3b9864869b2e76bcf94f3.
Strike Gamaredon LNK_fcc66920	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is fcc66920c881704e49cdfe366c35888c.
Strike Gamaredon LNK_ff5ee968	This strike sends a malware sample known as Gamaredon LNK. This malware sample was seen during attacks where the Gamaredon threat actor group targeted Ukrainian users with malicious LNK files to deliver the Remcos backdoor. The MD5 hash of this Gamaredon LNK sample is ff5ee968d208781635596ca0a75e618d.
Strike Gamarue_01d30b58	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is 01d30b58ced0722029bf33d9c8380aed.
Strike Gamarue_0bcb4a2d	This strike sends a polymorphic malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Gamarue sample is 0bcb4a2d2efa5f211f5d9dc4aac1246a.
Strike Gamarue_0dc48d5d	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is 0dc48d5d1bd8637abbaa22a7c2628b3a.
Strike Gamarue_0f2af894	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is 0f2af89460de5fe7331967d5f71a0bb9.

<b>Name</b>	<b>Description</b>
Strike Gamarue_11c69541	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is 11c695418eadfc9c1c6e83a538bc30a6.
Strike Gamarue_28a8fa22	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is 28a8fa223f15bd707365602b9d07c409.
Strike Gamarue_3109f7b5	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is 3109f7b5e2b3feb06e6876797ca5b964.
Strike Gamarue_3861c6df	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is 3861c6df0f2c6ceba149bc09e51509b7.
Strike Gamarue_51b30f40	This strike sends a polymorphic malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Gamarue sample is 51b30f403012636119e3b5fdacfa74f9.
Strike Gamarue_7df6bd24	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is 7df6bd248b00fe3458591c996ca969fd.

<b>Name</b>	<b>Description</b>
Strike Gamarue_84071b13	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is 84071b13ac60297978051069223b60c0.
Strike Gamarue_89a1e176	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is 89a1e176858e569ef99593d7f58929ec.
Strike Gamarue_9681ced1	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is 9681ced1fbff560cd894d2785639ca51.
Strike Gamarue_a208ad70	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is a208ad7018437136b64d2f4c1af7c747.
Strike Gamarue_aef60c6d	This strike sends a polymorphic malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The binary has random bytes appended at the end of the file. The MD5 hash of this Gamarue sample is aef60c6d7f959e086091da6e009bf27d.
Strike Gamarue_bae65735	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is bae6573551f8db9dff7435e48c237c7f.
Strike Gamarue_c53222ea	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is c53222eacadfe39272f6fcf3303c2e98.

<b>Name</b>	<b>Description</b>
Strike Gamarue_cca88bd6	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is cca88bd68a1ba8bfdca268cace9a27f6.
Strike Gamarue_d55fe6fa	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is d55fe6fa8d2ba3c2c6300a71990f38c2.
Strike Gamarue_e3752433	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is e3752433d62f4dbf29345aa5ecacafa9.
Strike Gamarue_e438a983	This strike sends a polymorphic malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Gamarue sample is e438a983fb2dc274d39702d4a860df15.
Strike Gamarue_e8c5bb4f	This strike sends a polymorphic malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Gamarue sample is e8c5bb4f6d9ed4ec046cb8989dba860e.
Strike Gamarue_e9ec1a06	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is e9ec1a063f0d557bfec2b04153b20cbe.

<b>Name</b>	<b>Description</b>
Strike Gamarue_fde8fb71	This strike sends a malware sample known as Gamarue. Win.Trojan.Gamarue covers a family that, after installing itself on the system to survive after reboot, will spread itself to USB drives and modify system configuration settings to weaken its security and disable certain features, such as the task manager or the Windows shell, in order to protect itself. It can exfiltrate sensitive data and receive additional commands. The MD5 hash of this Gamarue sample is fde8fb71e98e02c81f20004bba7919f7.
Strike Gandcrab_1c6b014e	This strike sends a malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The MD5 hash of this Gandcrab sample is 1c6b014e86d887ef235adbcdce8c23a7f.
Strike Gandcrab_22bc40bd	This strike sends a malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The MD5 hash of this Gandcrab sample is 22bc40bd16d93b14848a4e49b708c8a0.
Strike Gandcrab_6704dc8f	This strike sends a polymorphic malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Gandcrab sample is 6704dc8f351350724184257996f9066b.
Strike Gandcrab_7dc8699e	This strike sends a malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The MD5 hash of this Gandcrab sample is 7dc8699e71e067f3cd4600c2c4fd4a9f.
Strike Gandcrab_81740cc0	This strike sends a malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The MD5 hash of this Gandcrab sample is 81740cc0d01c2b9841f1946dadab4263.
Strike Gandcrab_8b73329e	This strike sends a malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The MD5 hash of this Gandcrab sample is 8b73329e7fbe4ea24e9b814c6fe3c61d.

<b>Name</b>	<b>Description</b>
Strike Gandcrab_9bfb2b63	This strike sends a polymorphic malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Gandcrab sample is 9bfb2b6312ba962055b988777e1ee99c.
Strike Gandcrab_9c8a7882	This strike sends a polymorphic malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Gandcrab sample is 9c8a788266cf8884798ea6bf37b1b10.
Strike Gandcrab_a01269b3	This strike sends a malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The MD5 hash of this Gandcrab sample is a01269b36a5f153ef7c210001e2b071a.
Strike Gandcrab_a1458bf8	This strike sends a malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The MD5 hash of this Gandcrab sample is a1458bf8e676667471b8ebddc42123ab.
Strike Gandcrab_a2ea3a19	This strike sends a malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The MD5 hash of this Gandcrab sample is a2ea3a1987942abe4d79b75d8676d2ad.
Strike Gandcrab_c78096f0	This strike sends a malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The MD5 hash of this Gandcrab sample is c78096f041d994cc2e007a1a0c09a357.
Strike Gandcrab_dd6e6968	This strike sends a malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The MD5 hash of this Gandcrab sample is dd6e6968b41bfe67b1eb6ca06009e029.

<b>Name</b>	<b>Description</b>
Strike Gandcrab_e34a5f17	This strike sends a malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The MD5 hash of this Gandcrab sample is e34a5f177d5bb5b8012024708d3f0217.
Strike Gandcrab_e45f0c5d	This strike sends a malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The MD5 hash of this Gandcrab sample is e45f0c5d59ce9f66ecbf7f1207e010fc.
Strike Gandcrab_e7a61e47	This strike sends a polymorphic malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Gandcrab sample is e7a61e4706cc30fd9fce858d4461a7fb.
Strike Gandcrab_eb5f7771	This strike sends a malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The MD5 hash of this Gandcrab sample is eb5f77715eb2a50f1aa03074f3ad388.
Strike Gandcrab_fc157cd5	This strike sends a malware sample known as Gandcrab. GandCrab is ransomware that encrypts documents, photos, databases and other important files typically using the file extension ".GDCB," ".CRAB" or ".KRAB." GandCrab is spread through both traditional spam campaigns, as well as multiple exploit kits, including Rig and GrandSoft. The MD5 hash of this Gandcrab sample is fc157cd5d8a9c32ecaec8a273b064296.
Strike GayFemBoy_03ac6a68	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 03ac6a687be22b30ec48656235fef107.
Strike GayFemBoy_07025e99	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 07025e9990963038249ff2b771ee5d5c.

<b>Name</b>	<b>Description</b>
Strike GayFemBoy_0b6e8d5d	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 0b6e8d5d68dda316da6125d8f6b6ced3.
Strike GayFemBoy_0e17f987	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 0e17f987efa46626eb5d22d6516b3718.
Strike GayFemBoy_100d33b8	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 100d33b8167c0c7d842f0cd93f01648b.
Strike GayFemBoy_12b4f549	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 12b4f549ae5e131f01b0b1181b06c71e.
Strike GayFemBoy_1e715cf1	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 1e715cf11e649b8e294d7877e9ce033b.
Strike GayFemBoy_1e728e64	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 1e728e6439296e9442db6fbcb488bedc.

<b>Name</b>	<b>Description</b>
Strike GayFemBoy_22e99928	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 22e99928283dd4cf0d8de14511ef752d.
Strike GayFemBoy_28343b78	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 28343b780bf5d8b9e6b7a274418f997f.
Strike GayFemBoy_3246002d	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 3246002d1f2e0506af4d13e6847d3a60.
Strike GayFemBoy_431dbc9e	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 431dbc9e8e1b6cad13f5843fd3ea18b9.
Strike GayFemBoy_4408fca1	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 4408fca1a089360be769be08000fc5a1.
Strike GayFemBoy_513c7b85	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 513c7b85dfa334c0239a6446f88e148c.

<b>Name</b>	<b>Description</b>
Strike GayFemBoy_5e1a6c16	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 5e1a6c16bee32894b4b950d9eac58192.
Strike GayFemBoy_6259fe5c	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 6259fe5c02fbbb702a85c557627af242.
Strike GayFemBoy_648375d6	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 648375d6acd2e0997a7492f2afbdd878.
Strike GayFemBoy_64f9bb8d	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 64f9bb8df99874eca578f0ce9744aad1.
Strike GayFemBoy_69b85867	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 69b85867eca0e3bd7cafd4e3f192c0a8.
Strike GayFemBoy_6e7d22a1	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 6e7d22a17f5534aea0b45f01a008e745.

<b>Name</b>	<b>Description</b>
Strike GayFemBoy_6fad431b	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 6fad431b9d6b5259127fb1e57d23fb87.
Strike GayFemBoy_96946e70	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 96946e70c541e54f352bad8c3fa24b1a.
Strike GayFemBoy_9b31ff6a	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 9b31ff6a02b18bafec874c51a1d2321a.
Strike GayFemBoy_9d10f85e	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is 9d10f85e8aaa077b39742f8a54bd75ab.
Strike GayFemBoy_a0a0503b	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is a0a0503bf342c4f82e1aefbf28224550.
Strike GayFemBoy_a166c743	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is a166c743a0141ee18fa912768b767410.

<b>Name</b>	<b>Description</b>
Strike GayFemBoy_a23acaf1	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is a23acaf15e11a623827b44e30ef8c56d.
Strike GayFemBoy_aedae14b	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is aedae14b13971c2f9cf8963c2e6e6667.
Strike GayFemBoy_b1c2b561	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is b1c2b561dd2eae64d89988438bde2639.
Strike GayFemBoy_b9953c35	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is b9953c35f94b231a5e05f818c978c6e2.
Strike GayFemBoy_bd9aecbf	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is bd9aecbfbe099ec9c62873f794b410c5.
Strike GayFemBoy_caee37ae	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is caee37aec95686de5a033c6334e51799.

<b>Name</b>	<b>Description</b>
Strike GayFemBoy_d7df605f	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is d7df605f7ca64352f40293edc59b57f2.
Strike GayFemBoy_da734b14	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is da734b14aac135abce426ab603b6fb6.
Strike GayFemBoy_f92e579f	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is f92e579f058de6f19d5c40dff1aeb3b2.
Strike GayFemBoy_ff296fc2	This strike sends a malware sample known as GayFemBoy. GayFemBoy is a malware of the Mirai botnet family that targets IoT devices, particularly DVRs/NVRs. It infects devices by exploiting known vulnerabilities or using default credentials. Once executed, the malware converts the infected devices into bots that can be used for DDoS attacks or to spread the malware further. Its key capabilities include launching DDoS attacks, self-replication, and the ability to execute arbitrary commands. The MD5 hash of this GayFemBoy sample is ff296fc2d3fc35edcbbeda8aefce75d7.
Strike Gh0stRAT_0f6550a7	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 0f6550a771aef1df84f85e95ff7adb9b.
Strike Gh0stRAT_10733ef1	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 10733ef18028d94596776413babaa9920.
Strike Gh0stRAT_16b909ea	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 16b909ea39f0a1f22a176bf3418ab148.

<b>Name</b>	<b>Description</b>
Strike Gh0stRAT_16c59693	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 16c596936a8c80d6d8810257527f377d.
Strike Gh0stRAT_2b65b00a	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 2b65b00a17cf1a52a6bd1514436681fd.
Strike Gh0stRAT_2be3fc0f	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 2be3fc0fc545426dffbb18de235b9418f.
Strike Gh0stRAT_2c10444b	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 2c10444bbe4c56ef89a26335ae4b74bb.
Strike Gh0stRAT_31a7ba62	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 31a7ba6276ad876d12d537c8f4076d14.
Strike Gh0stRAT_34a648b5	This strike sends a polymorphic malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The binary has random bytes appended at the end of the file. The MD5 hash of this Gh0stRAT sample is 34a648b57683dd4d48a4123aee6542be.
Strike Gh0stRAT_38db1ea3	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 38db1ea30d13a611098c91721bd7daeb.
Strike Gh0stRAT_3d895086	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 3d89508646d71122137fc8576191f1dc.

<b>Name</b>	<b>Description</b>
Strike Gh0stRAT_46fda509	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 46fda5099af718be6fec6710916decb8.
Strike Gh0stRAT_4793b3b8	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 4793b3b82cd0ad256572aff6109f78f5.
Strike Gh0stRAT_52729f8b	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 52729f8b7185d792be872d0821a251a0.
Strike Gh0stRAT_5544f188	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 5544f188c207c2b04e07f9f74f18874b.
Strike Gh0stRAT_572f5ee8	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 572f5ee8ebf9b86c48906dbbb928a78a.
Strike Gh0stRAT_58db1853	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 58db185381561f59c85b0f5eccb428af.
Strike Gh0stRAT_596fcbea	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 596fcbea1a5f3fa86bcf5039881aa576.
Strike Gh0stRAT_5b99f7d1	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 5b99f7d15824fc12df2c4400fe57a492.
Strike Gh0stRAT_6524e285	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 6524e285d22bb93b6cf2f210c6b9eb7b.

<b>Name</b>	<b>Description</b>
Strike Gh0stRAT_65a69489	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 65a69489423b963beee69ad1b7644c49.
Strike Gh0stRAT_7aef37ac	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 7aef37acaf6da745135659e0903dc5d5.
Strike Gh0stRAT_8068c7ce	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 8068c7ce20d94bdf1d843c98e916a009.
Strike Gh0stRAT_84de5fb9	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 84de5fb9b9067e63fd51f44777d898f0.
Strike Gh0stRAT_8acac9bc	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 8acac9bca9605fc425aaeeba1d90c19a.
Strike Gh0stRAT_8f223f8f	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 8f223f8fba761d9d15d1a842eaecedaf.
Strike Gh0stRAT_8fe74bf9	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 8fe74bf9a3b754612869be86468b432f.
Strike Gh0stRAT_90b4b512	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 90b4b51248d5d633fa688663b5198284.
Strike Gh0stRAT_9a04833e	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is 9a04833e6ac8a5bf621fcc492e88ee83.

<b>Name</b>	<b>Description</b>
Strike Gh0stRAT_a244251c	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is a244251c91ddaa4838a0642b36e703e6.
Strike Gh0stRAT_a5d16fe0	This strike sends a polymorphic malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Gh0stRAT sample is a5d16fe034462a43c0ddb0b62a52121e.
Strike Gh0stRAT_a61ffb11	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is a61ffb1143f1c6bf04d41dff02e93ede.
Strike Gh0stRAT_a872d440	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is a872d44042b1ca69c033a89657d60c27.
Strike Gh0stRAT_ab8205af	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is ab8205af204ef7cbf98a20ee0fdb4960.
Strike Gh0stRAT_ac8b5f9b	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is ac8b5f9b4ad83be4f596bb5c953f1dd8.
Strike Gh0stRAT_b11e4378	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is b11e4378225a2a99a988621260902551.
Strike Gh0stRAT_b170ba52	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is b170ba528f2ade834483f410b22fd910.

<b>Name</b>	<b>Description</b>
Strike Gh0stRAT_b3869d2e	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is b3869d2e835647c3081587f8b9cd7eab.
Strike Gh0stRAT_b56ebb9a	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is b56ebb9adf9bc7f6105082f9b9d93b3b.
Strike Gh0stRAT_b5b8cfa2	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is b5b8cfa2a4e8978f64149d17da577b6d.
Strike Gh0stRAT_b640f7ed	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is b640f7ed51715ed04cf89f794e5ae924.
Strike Gh0stRAT_b7d08f31	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is b7d08f31c8ec29a6273035e657ce3afa.
Strike Gh0stRAT_bc93f615	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is bc93f6154632f07d17bf00e82849201d.
Strike Gh0stRAT_bd3b1251	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is bd3b12515725e179f1e4678223066247.
Strike Gh0stRAT_be41f5c4	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is be41f5c41e8594602a405b72a5b23060.
Strike Gh0stRAT_c0835179	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is c083517967757144fafbb58bf094d240.

<b>Name</b>	<b>Description</b>
Strike Gh0stRAT_cb107719	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is cb1077195da0ed778a3180ab0aaf4c92.
Strike Gh0stRAT_cfbfe8a	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is cfbfe8ae5f45d5cc06bd15f639397e4.
Strike Gh0stRAT_d07af306	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is d07af306f18422cc1f258ec115d16df8.
Strike Gh0stRAT_d1c7d9b6	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is d1c7d9b619ac682d4d3c4635b2b4ed5a.
Strike Gh0stRAT_d2a67090	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is d2a67090e3a8b6d1ca55ff3f3f00c768.
Strike Gh0stRAT_e3d7e295	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is e3d7e295c9c494cf73c46cc58e5c32d.
Strike Gh0stRAT_e80c46e8	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is e80c46e8291322e25085beded0fca16a.
Strike Gh0stRAT_e9694748	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is e969474837b9cd28ffbc4f1ffc62e973.
Strike Gh0stRAT_eba0031e	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is eba0031e564ce3b9d7c37bb4f9648480.

<b>Name</b>	<b>Description</b>
Strike Gh0stRAT_f05288d0	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is f05288d0c72b65c0cf71852454a17fcf.
Strike Gh0stRAT_f2c25eab	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is f2c25eab5b6be1a11948729709af7da6.
Strike Gh0stRAT_f7031eeb	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is f7031eeb4c7a87b72cd6432524e46849.
Strike Gh0stRAT_f748ba45	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is f748ba45b2c32e82ab5c3df7d649e7d0.
Strike Gh0stRAT_f9c41e77	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is f9c41e775ffc495c2afaf795acc3d4eb.
Strike Gh0stRAT_fb38fdbf	This strike sends a malware sample known as Gh0stRAT. Gh0stRAT is a remote access Trojan that provides control over an infected system. Some of its known functions include the ability to record keystrokes, record screenshots and download additional malicious payloads. The MD5 hash of this Gh0stRAT sample is fb38fdbf6527cfa784a8f9d6dde56a3f.
Strike GhostCall_0af11f61	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 0af11f610da1f691e43173d44643283f.
Strike GhostCall_12439688	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 1243968876262c3ad4250e1371447b23.

<b>Name</b>	<b>Description</b>
Strike GhostCall_5ad40a5f	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 5ad40a5fd18a1b57b69c44bc2963dc6b.
Strike GhostCall_6348b49f	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 6348b49f3499d760797247b94385fda3.
Strike GhostCall_76ace3a6	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 76ace3a6892c25512b17ed42ac2ebd05.
Strike GhostCall_931cec3c	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 931cec3c80c78d233e3602a042a2e71b.
Strike GhostCall_9551b4af	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 9551b4af789b2db563f9452eaf46b6aa.
Strike GhostCall_963f473f	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is 963f473f1734d8b3fbb8c9a227c06d07.

<b>Name</b>	<b>Description</b>
Strike GhostCall_c42c7a2e	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is c42c7a2ea1c2f00dddb0cc4c8fb5bcf.
Strike GhostCall_c446682f	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is c446682f33641cff21083ac2ce477dbe.
Strike GhostCall_d8529855	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is d8529855fab4b4aa6c2b34449cb3b9fb.
Strike GhostCall_e33f942c	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is e33f942cf1479ca8530a916868bad954.
Strike GhostCall_e8680d17	This strike sends a malware sample known as GhostCall. GhostCall is a malware that is used for cyber espionage activities. It is delivered via spear-phishing emails containing malicious HWP (Hangul Word Processor) documents. Upon opening the document, a malicious payload is dropped and executed which then communicates with a command and control server. The malware's key capabilities include stealing information, maintaining persistence, and bypassing antivirus detection. The MD5 hash of this GhostCall sample is e8680d17fba6425e4a9bb552fb8db2b1.
Strike GhostLocker_00c69252	This strike sends a malware sample known as GhostLocker. GhostLocker is a Ransomware-as-a-Service encryptor introduced by a hacktivist group GhostSec. It targets telecommunications companies, surveillance systems, and IoT devices, marketing itself as an enterprise-grade locking software prioritizing safety and effectiveness. Key features include military-grade encryption, undetectability through a polymorphic stub, protection against reverse engineering, self-deletion, service termination, automatic privilege escalation, persistence, a watchdog process, and delayed encryption. The MD5 hash of this GhostLocker sample is 00c69252bc0e896e2a8b0a9a3d68e41e.

Name	Description
Strike GhostLocker_4119af0c	This strike sends a malware sample known as GhostLocker. GhostLocker is a Ransomware-as-a-Service encryptor introduced by a hacktivist group GhostSec. It targets telecommunications companies, surveillance systems, and IoT devices, marketing itself as an enterprise-grade locking software prioritizing safety and effectiveness. Key features include military-grade encryption, undetectability through a polymorphic stub, protection against reverse engineering, self-deletion, service termination, automatic privilege escalation, persistence, a watchdog process, and delayed encryption. The MD5 hash of this GhostLocker sample is 4119af0c5a12d6153e19514b4be993c4.
Strike GhostLocker_81a13602	This strike sends a malware sample known as GhostLocker. GhostLocker is a Ransomware-as-a-Service encryptor introduced by a hacktivist group GhostSec. It targets telecommunications companies, surveillance systems, and IoT devices, marketing itself as an enterprise-grade locking software prioritizing safety and effectiveness. Key features include military-grade encryption, undetectability through a polymorphic stub, protection against reverse engineering, self-deletion, service termination, automatic privilege escalation, persistence, a watchdog process, and delayed encryption. The MD5 hash of this GhostLocker sample is 81a136029d29d26920c0287faf778776.
Strike GhostLocker_8506b32e	This strike sends a malware sample known as GhostLocker. GhostLocker is a Ransomware-as-a-Service encryptor introduced by a hacktivist group GhostSec. It targets telecommunications companies, surveillance systems, and IoT devices, marketing itself as an enterprise-grade locking software prioritizing safety and effectiveness. Key features include military-grade encryption, undetectability through a polymorphic stub, protection against reverse engineering, self-deletion, service termination, automatic privilege escalation, persistence, a watchdog process, and delayed encryption. The MD5 hash of this GhostLocker sample is 8506b32ea38dc3a844e72051750a75d9.
Strike GhostLocker_9c66d8fd	This strike sends a malware sample known as GhostLocker. GhostLocker is a Ransomware-as-a-Service encryptor introduced by a hacktivist group GhostSec. It targets telecommunications companies, surveillance systems, and IoT devices, marketing itself as an enterprise-grade locking software prioritizing safety and effectiveness. Key features include military-grade encryption, undetectability through a polymorphic stub, protection against reverse engineering, self-deletion, service termination, automatic privilege escalation, persistence, a watchdog process, and delayed encryption. The MD5 hash of this GhostLocker sample is 9c66d8fde4e6d395558182156e6fe298.
Strike GhostLocker_bdc119ef	This strike sends a malware sample known as GhostLocker. GhostLocker is a Ransomware-as-a-Service encryptor introduced by a hacktivist group GhostSec. It targets telecommunications companies, surveillance systems, and IoT devices, marketing itself as an enterprise-grade locking software prioritizing safety and effectiveness. Key features include military-grade encryption, undetectability through a polymorphic stub, protection against reverse engineering, self-deletion, service termination, automatic privilege escalation, persistence, a watchdog process, and delayed encryption. The MD5 hash of this GhostLocker sample is bdc119efae38ea528c10adbd4c9000e4.

<b>Name</b>	<b>Description</b>
Strike GhostLocker_bea3d03f	This strike sends a malware sample known as GhostLocker. GhostLocker is a Ransomware-as-a-Service encryptor introduced by a hacktivist group GhostSec. It targets telecommunications companies, surveillance systems, and IoT devices, marketing itself as an enterprise-grade locking software prioritizing safety and effectiveness. Key features include military-grade encryption, undetectability through a polymorphic stub, protection against reverse engineering, self-deletion, service termination, automatic privilege escalation, persistence, a watchdog process, and delayed encryption. The MD5 hash of this GhostLocker sample is bea3d03f686c73622f08b1f0f8ec5b43.
Strike GhostLocker_cd906ad0	This strike sends a malware sample known as GhostLocker. GhostLocker is a Ransomware-as-a-Service encryptor introduced by a hacktivist group GhostSec. It targets telecommunications companies, surveillance systems, and IoT devices, marketing itself as an enterprise-grade locking software prioritizing safety and effectiveness. Key features include military-grade encryption, undetectability through a polymorphic stub, protection against reverse engineering, self-deletion, service termination, automatic privilege escalation, persistence, a watchdog process, and delayed encryption. The MD5 hash of this GhostLocker sample is cd906ad0553a176d8737b4b85109687c.
Strike GhostLocker_dfb5e296	This strike sends a malware sample known as GhostLocker. GhostLocker is a Ransomware-as-a-Service encryptor introduced by a hacktivist group GhostSec. It targets telecommunications companies, surveillance systems, and IoT devices, marketing itself as an enterprise-grade locking software prioritizing safety and effectiveness. Key features include military-grade encryption, undetectability through a polymorphic stub, protection against reverse engineering, self-deletion, service termination, automatic privilege escalation, persistence, a watchdog process, and delayed encryption. The MD5 hash of this GhostLocker sample is dfb5e2963e9bc48c904f4ac5978fe9ea.
Strike GhostLocker_dfbaa667	This strike sends a malware sample known as GhostLocker. GhostLocker is a Ransomware-as-a-Service encryptor introduced by a hacktivist group GhostSec. It targets telecommunications companies, surveillance systems, and IoT devices, marketing itself as an enterprise-grade locking software prioritizing safety and effectiveness. Key features include military-grade encryption, undetectability through a polymorphic stub, protection against reverse engineering, self-deletion, service termination, automatic privilege escalation, persistence, a watchdog process, and delayed encryption. The MD5 hash of this GhostLocker sample is dfbaa667c07fdd5ad2543ce98d097027.
Strike GhostLocker_e6ec894f	This strike sends a malware sample known as GhostLocker. GhostLocker is a Ransomware-as-a-Service encryptor introduced by a hacktivist group GhostSec. It targets telecommunications companies, surveillance systems, and IoT devices, marketing itself as an enterprise-grade locking software prioritizing safety and effectiveness. Key features include military-grade encryption, undetectability through a polymorphic stub, protection against reverse engineering, self-deletion, service termination, automatic privilege escalation, persistence, a watchdog process, and delayed encryption. The MD5 hash of this GhostLocker sample is e6ec894f69899d14e3e8581939fe0685.

<b>Name</b>	<b>Description</b>
Strike Gigabud RAT_b2429371	This strike sends a malware sample known as Gigabud RAT. Gigabud is a Remote Access Trojan Android malware that has been detected in the wild masquerading as government agencies, shopping apps, and banking applications from Thailand, the Philippines and Peru. The malware has many functions like the ability to receive commands from C2 servers, screen recording, and stealing banking credentials. The MD5 hash of this Gigabud RAT sample is b2429371b530d634b2b86c331515904f.
Strike Gigabud RAT_ca6aa6c5	This strike sends a malware sample known as Gigabud RAT. Gigabud is a Remote Access Trojan Android malware that has been detected in the wild masquerading as government agencies, shopping apps, and banking applications from Thailand, the Philippines and Peru. The malware has many functions like the ability to receive commands from C2 servers, screen recording, and stealing banking credentials. The MD5 hash of this Gigabud RAT sample is ca6aa6c5a7910281a899695e61423079.
Strike GoBear_0db6426b	This strike sends a polymorphic malware sample known as GoBear. GoBear is a Go based backdoor developed by the North Korean group Springtail. The binary has random bytes appended at the end of the file. The MD5 hash of this GoBear sample is 0db6426b2861a8f76bf95616eee9dd55.
Strike GoBear_418e4122	This strike sends a polymorphic malware sample known as GoBear. GoBear is a Go based backdoor developed by the North Korean group Springtail. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this GoBear sample is 418e4122cde54977c4851de04d10a9dc.
Strike GoBear_4a78dc18	This strike sends a polymorphic malware sample known as GoBear. GoBear is a Go based backdoor developed by the North Korean group Springtail. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this GoBear sample is 4a78dc18285aec436b80f07660563259.
Strike GoBear_54392569	This strike sends a polymorphic malware sample known as GoBear. GoBear is a Go based backdoor developed by the North Korean group Springtail. The binary has the checksum removed in the PE file format. The MD5 hash of this GoBear sample is 543925691e7d8d18bb10ef0e888afde7.
Strike GoBear_b74efd84	This strike sends a malware sample known as GoBear. GoBear is a Go based backdoor developed by the North Korean group Springtail. The MD5 hash of this GoBear sample is b74efd8470206a20175d723c14c2e872.
Strike GoBear_f423d4cc	This strike sends a polymorphic malware sample known as GoBear. GoBear is a Go based backdoor developed by the North Korean group Springtail. The binary has the signature removed in the PE file format. The MD5 hash of this GoBear sample is f423d4cc9d241347056ad62e48a3a25c.

<b>Name</b>	<b>Description</b>
Strike GoBruteforcer IRC_207d8d84	This strike sends a malware sample known as GoBruteforcer IRC. GoBruteforcer is malware written in Golang that targets web servers that run the phpMyAdmin, MySQL, FTP and Postgres services. This malware has support for x86,x64, and ARM processor architectures. Once the malware identifies a target it attempts to brute force one of the services listed above. After successfully doing so, it deploys an IRC bot as a method of communicating back to the attacker. The malware also can make attempts to communicate with the command and control server via a PHP web shell. These files are the IRC bot associated with GoBruteforcer. The MD5 hash of this GoBruteforcer IRC sample is 207d8d8496f174396849c8514ce28bee.
Strike GoBruteforcer Webshell_45172413	This strike sends a malware sample known as GoBruteforcer Webshell. GoBruteforcer is malware written in Golang that targets web servers that run the phpMyAdmin, MySQL, FTP and Postgres services. This malware has support for x86,x64, and ARM processor architectures. Once the malware identifies a target it attempts to brute force one of the services listed above. After successfully doing so, it deploys an IRC bot as a method of communicating back to the attacker. The malware also can make attempts to communicate with the command and control server via a PHP web shell. These files are Web shells associated with GoBruteforcer. The MD5 hash of this GoBruteforcer Webshell sample is 45172413e29114dc3820d7e5e2b08b4b.
Strike GoBruteforcer Webshell_c271f586	This strike sends a malware sample known as GoBruteforcer Webshell. GoBruteforcer is malware written in Golang that targets web servers that run the phpMyAdmin, MySQL, FTP and Postgres services. This malware has support for x86,x64, and ARM processor architectures. Once the malware identifies a target it attempts to brute force one of the services listed above. After successfully doing so, it deploys an IRC bot as a method of communicating back to the attacker. The malware also can make attempts to communicate with the command and control server via a PHP web shell. These files are Web shells associated with GoBruteforcer. The MD5 hash of this GoBruteforcer Webshell sample is c271f586d574e6f2ad87e9339835b172.
Strike GoBruteforcer_8f56aeb3	This strike sends a malware sample known as GoBruteforcer. GoBruteforcer is malware written in Golang that targets web servers that run the phpMyAdmin, MySQL, FTP and Postgres services. This malware has support for x86,x64, and ARM processor architectures. Once the malware identifies a target it attempts to brute force one of the services listed above. After successfully doing so, it deploys an IRC bot as a method of communicating back to the attacker. The malware also can make attempts to communicate with the command and control server via a PHP web shell. This file is the GoBruteforcer malware. The MD5 hash of this GoBruteforcer sample is 8f56aeb3d516e6deb858a73da66e1071.
Strike GoBruteforcer_b6134c83	This strike sends a malware sample known as GoBruteforcer. GoBruteforcer is malware written in Golang that targets web servers that run the phpMyAdmin, MySQL, FTP and Postgres services. This malware has support for x86,x64, and ARM processor architectures. Once the malware identifies a target it attempts to brute force one of the services listed above. After successfully doing so, it deploys an IRC bot as a method of communicating back to the attacker. The malware also can make attempts to communicate with the command and control server via a PHP web shell. This file is the GoBruteforcer malware. The MD5 hash of this GoBruteforcer sample is b6134c83fbb3ef6fdff045463038969a.

<b>Name</b>	<b>Description</b>
Strike GoBruteforcer_ffeb1d82	This strike sends a malware sample known as GoBruteforcer. GoBruteforcer is malware written in Golang that targets web servers that run the phpMyAdmin, MySQL, FTP and Postgres services. This malware has support for x86,x64, and ARM processor architectures. Once the malware identifies a target it attempts to brute force one of the services listed above. After successfully doing so, it deploys an IRC bot as a method of communicating back to the attacker. The malware also can make attempts to communicate with the command and control server via a PHP web shell. This file is the GoBruteforcer malware. The MD5 hash of this GoBruteforcer sample is ffeb1d82987d745daf3c9e59f7ce7d37.
Strike GoatRAT_ba5833b4	This strike sends a malware sample known as GoatRAT. GoatRAT is an Android banking trojan. This malware tool attempts to communicate with a C2 server to obtain a PIX Key to perform fraudulent money transactions. This is carried out by employing the ATS or Automated Transfer System technique where a user logs into a banking app and the malware controls the transfers. The MD5 hash of this GoatRAT sample is ba5833b49e2c6501f5bbce90b7948a85.
Strike Godfather_3910e0f2	This strike sends an Android malware sample known as Godfather. It is a trojan which affected 400 banking and crypto applications. It is a successor to the Anubis malware which performs its C2 communication over telegram and does malicious activities like screen recording, exfiltrates push notifications for bypassing 2FA, forwards calls etc. The included sample poses as the Google Play Protect app. The MD5 hash of this Godfather sample is 3910e0f2fa87ef1ac40098c98709886d.
Strike Godfather_7e061e87	This strike sends a malware sample known as Godfather. This strike sends an Android malware sample known as Godfather. It is a trojan which affected 400 banking and crypto applications. It is a successor to the Anubis malware which performs its C2 communication over telegram and does malicious activities like screen recording, exfiltrates push notifications for bypassing 2FA, forwards calls etc. The included sample poses as the Google Play Protect app. The MD5 hash of this Godfather sample is 7e061e87f9a4c27bfb69980980270720.
Strike Godfather_87cc15bb	This strike sends an Android malware sample known as Godfather. It is a trojan which affected 400 banking and crypto applications. It is a successor to the Anubis malware which performs its C2 communication over telegram and does malicious activities like screen recording, exfiltrates push notifications for bypassing 2FA, forwards calls etc. The included sample poses as the Google Play Protect app. The MD5 hash of this Godfather sample is 87cc15bb3d8481c3b9f635a24cdfecee.
Strike Grayling_092479f5	This strike sends a malware sample known as Grayling. This sample belongs to a campaign called Grayling. It uses public infrastructure for initial access, deploying shells, and involves a DLL sideloading attack through API SbieDll_Hook and other loading tools. On gaining access attackers escalate privileges, scan networks, and employ downloaders. The MD5 hash of this Grayling sample is 092479f5e1a584e89b8e03ccace849bd.

<b>Name</b>	<b>Description</b>
Strike Grayling_1ba885f6	This strike sends a malware sample known as Grayling. This sample belongs to a campaign called Grayling. It uses public infrastructure for initial access, deploying shells, and involves a DLL sideloading attack through API SbieDll_Hook and other loading tools. On gaining access attackers escalate privileges, scan networks, and employ downloaders. The MD5 hash of this Grayling sample is 1ba885f6c185b2ec822d831bcc77949.
Strike Grayling_24137ac3	This strike sends a malware sample known as Grayling. This sample belongs to a campaign called Grayling. It uses public infrastructure for initial access, deploying shells, and involves a DLL sideloading attack through API SbieDll_Hook and other loading tools. On gaining access attackers escalate privileges, scan networks, and employ downloaders. The MD5 hash of this Grayling sample is 24137ac3dcad6a12abd58611a5d0c8b9.
Strike Grayling_3c73150f	This strike sends a malware sample known as Grayling. This sample belongs to a campaign called Grayling. It uses public infrastructure for initial access, deploying shells, and involves a DLL sideloading attack through API SbieDll_Hook and other loading tools. On gaining access attackers escalate privileges, scan networks, and employ downloaders. The MD5 hash of this Grayling sample is 3c73150fbc80de0019e614c30c7206af.
Strike Grayling_469c57f7	This strike sends a malware sample known as Grayling. This sample belongs to a campaign called Grayling. It uses public infrastructure for initial access, deploying shells, and involves a DLL sideloading attack through API SbieDll_Hook and other loading tools. On gaining access attackers escalate privileges, scan networks, and employ downloaders. The MD5 hash of this Grayling sample is 469c57f7448e3884b4f11f652c45c38f.
Strike Grayling_606d786a	This strike sends a malware sample known as Grayling. This sample belongs to a campaign called Grayling. It uses public infrastructure for initial access, deploying shells, and involves a DLL sideloading attack through API SbieDll_Hook and other loading tools. On gaining access attackers escalate privileges, scan networks, and employ downloaders. The MD5 hash of this Grayling sample is 606d786a265ae7102255027b044432cf.
Strike Grayling_a49ee90e	This strike sends a malware sample known as Grayling. This sample belongs to a campaign called Grayling. It uses public infrastructure for initial access, deploying shells, and involves a DLL sideloading attack through API SbieDll_Hook and other loading tools. On gaining access attackers escalate privileges, scan networks, and employ downloaders. The MD5 hash of this Grayling sample is a49ee90ee45bcb717b1e65facf8f8ce3.
Strike Grayling_a9833509	This strike sends a malware sample known as Grayling. This sample belongs to a campaign called Grayling. It uses public infrastructure for initial access, deploying shells, and involves a DLL sideloading attack through API SbieDll_Hook and other loading tools. On gaining access attackers escalate privileges, scan networks, and employ downloaders. The MD5 hash of this Grayling sample is a983350925f47c7e50d2ddbe0fec695f.
Strike Grayling_b6a63b62	This strike sends a malware sample known as Grayling. This sample belongs to a campaign called Grayling. It uses public infrastructure for initial access, deploying shells, and involves a DLL sideloading attack through API SbieDll_Hook and other loading tools. On gaining access attackers escalate privileges, scan networks, and employ downloaders. The MD5 hash of this Grayling sample is b6a63b6250dcebdc112729cc2311a80.

<b>Name</b>	<b>Description</b>
Strike Grayling_c720aff8	This strike sends a malware sample known as Grayling. This sample belongs to a campaign called Grayling. It uses public infrastructure for initial access, deploying shells, and involves a DLL sideloading attack through API SbieDll_Hook and other loading tools. On gaining access attackers escalate privileges, scan networks, and employ downloaders. The MD5 hash of this Grayling sample is c720aff8f1c5a34fb4f0c61ffaa47225.
Strike Grayling_c93d2c2d	This strike sends a malware sample known as Grayling. This sample belongs to a campaign called Grayling. It uses public infrastructure for initial access, deploying shells, and involves a DLL sideloading attack through API SbieDll_Hook and other loading tools. On gaining access attackers escalate privileges, scan networks, and employ downloaders. The MD5 hash of this Grayling sample is c93d2c2d8d9b51a6c1b778c7ddd40455.
Strike Grayling_f8a6759e	This strike sends a malware sample known as Grayling. This sample belongs to a campaign called Grayling. It uses public infrastructure for initial access, deploying shells, and involves a DLL sideloading attack through API SbieDll_Hook and other loading tools. On gaining access attackers escalate privileges, scan networks, and employ downloaders. The MD5 hash of this Grayling sample is f8a6759eebaea38f309f4560cbe52211.
Strike Greenbean_7c8ae6df	This strike sends a polymorphic malware sample known as Greenbean. Arid Viper is an espionage-driven group that delivers attacks targeting Middle Eastern Android users through social engineering techniques. Their primary tool is SpyC23, a family of Android malware disguised as legitimate applications. It steals sensitive information from the device, disables security notifications, and deploys additional malware. 'com.missdong' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 7c8ae6dfe6c41bc4f53feff31d5485b2.
Strike Greenbean_affdbcacf	This strike sends a polymorphic malware sample known as Greenbean. Arid Viper is an espionage-driven group that delivers attacks targeting Middle Eastern Android users through social engineering techniques. Their primary tool is SpyC23, a family of Android malware disguised as legitimate applications. It steals sensitive information from the device, disables security notifications, and deploys additional malware. 'com.missdong' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is affdbcacf76a2c6ae436a0ac29eda3e19.
Strike Greenbean_bf22b7f3	This strike sends a malware sample known as Greenbean. Arid Viper is an espionage-driven group that delivers attacks targeting Middle Eastern Android users through social engineering techniques. Their primary tool is SpyC23, a family of Android malware disguised as legitimate applications. It steals sensitive information from the device, disables security notifications, and deploys additional malware. 'com.missdong' is the package name of the malware sample. The MD5 hash of this malware sample is bf22b7f3a2136314b330f66b82c46123.

<b>Name</b>	<b>Description</b>
Strike Guerrilla_a03f9011	This strike sends a malware sample known as Guerrilla. This strike sends an Android malware sample known as Guerrilla. It is attributed to the threat actors in Lemon Group. The malware has a plugin based architecture which includes a SMS plugin capable of intercepting messages, proxy plugin, a silent plugin for silent app installations. 'zfi.kkvwej.cby.hpyz' is the package name of the malware sample. The MD5 hash of this Guerrilla sample is a03f901158375ca3e5062431ba2ca73f.
Strike HAFNIUM Webshell_1a7a85b0	This strike sends a malware sample known as HAFNIUM Webshell. This HAFNIUM Webshell malware is one of many that has been used in conjunction with Microsoft Exchange Server 0day attacks against a large number of entities primarily based in the United States. After initial infection these web shells are deployed, allowing attackers to steal data and perform further malicious functionality like command execution, file read/write capabilities and tunneling. The Webshell malware has been documented residing in one of several installation paths below. C:\inetpub\wwwroot\aspnet_client\ C:\inetpub\wwwroot\aspnet_client\system_web\ %PROGRAMFILES%\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\ C:\Exchange\FrontEnd\HttpProxy\owa\auth\ The MD5 hash of this HAFNIUM Webshell sample is 1a7a85b0390b308b1801679e11567eac.
Strike HAFNIUM Webshell_4b3039cf	This strike sends a malware sample known as HAFNIUM Webshell. This HAFNIUM Webshell malware is one of many that has been used in conjunction with Microsoft Exchange Server 0day attacks against a large number of entities primarily based in the United States. After initial infection these web shells are deployed, allowing attackers to steal data and perform further malicious functionality like command execution, file read/write capabilities and tunneling. The Webshell malware has been documented residing in one of several installation paths below. C:\inetpub\wwwroot\aspnet_client\ C:\inetpub\wwwroot\aspnet_client\system_web\ %PROGRAMFILES%\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\ C:\Exchange\FrontEnd\HttpProxy\owa\auth\ The MD5 hash of this HAFNIUM Webshell sample is 4b3039cf227c611c45d2242d1228a121.
Strike HAFNIUM Webshell_4ef04cba	This strike sends a malware sample known as HAFNIUM Webshell. This HAFNIUM Webshell malware is one of many that has been used in conjunction with Microsoft Exchange Server 0day attacks against a large number of entities primarily based in the United States. After initial infection these web shells are deployed, allowing attackers to steal data and perform further malicious functionality like command execution, file read/write capabilities and tunneling. The Webshell malware has been documented residing in one of several installation paths below. C:\inetpub\wwwroot\aspnet_client\ C:\inetpub\wwwroot\aspnet_client\system_web\ %PROGRAMFILES%\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\ C:\Exchange\FrontEnd\HttpProxy\owa\auth\ The MD5 hash of this HAFNIUM Webshell sample is 4ef04cba6bec2c3a164b9b755efbeb1c.

Name	Description
Strike HAFNIUM Webshell_5544ba9a	<p>This strike sends a malware sample known as HAFNIUM Webshell. This HAFNIUM Webshell malware is one of many that has been used in conjunction with Microsoft Exchange Server 0day attacks against a large number of entities primarily based in the United States. After initial infection these web shells are deployed, allowing attackers to steal data and perform further malicious functionality like command execution, file read/write capabilities and tunneling. The Webshell malware has been documented residing in one of several installation paths below. C:\inetpub\wwwroot\aspnet_client\ C:\inetpub\wwwroot\aspnet_client\system_web\ %PROGRAMFILES%\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\ C:\Exchange\FrontEnd\HttpProxy\owa\auth\ The MD5 hash of this HAFNIUM Webshell sample is 5544ba9ad1b56101b5d52b5270421d4a.</p>
Strike HAFNIUM Webshell_fe15fc63	<p>This strike sends a malware sample known as HAFNIUM Webshell. This HAFNIUM Webshell malware is one of many that has been used in conjunction with Microsoft Exchange Server 0day attacks against a large number of entities primarily based in the United States. After initial infection these web shells are deployed, allowing attackers to steal data and perform further malicious functionality like command execution, file read/write capabilities and tunneling. The Webshell malware has been documented residing in one of several installation paths below. C:\inetpub\wwwroot\aspnet_client\ C:\inetpub\wwwroot\aspnet_client\system_web\ %PROGRAMFILES%\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\ C:\Exchange\FrontEnd\HttpProxy\owa\auth\ The MD5 hash of this HAFNIUM Webshell sample is fe15fc6341baad2a111462854f96a2bc.</p>
Strike HZ_0c3201d0	<p>This strike sends a malware sample known as HZ. HZ is Remote Access Trojan backdoor. This is a macOS version of HZ that was has been associated with popular messaging apps like DingTalk and WeChat. The malware collects the victim information and communicates with a C2 server to execute additional commands. The MD5 hash of this HZ sample is 0c3201d0743c63075b18023bb8071e73.</p>
Strike HZ_287ccbf0	<p>This strike sends a malware sample known as HZ. HZ is Remote Access Trojan backdoor. This is a macOS version of HZ that was has been associated with popular messaging apps like DingTalk and WeChat. The malware collects the victim information and communicates with a C2 server to execute additional commands. The MD5 hash of this HZ sample is 287ccbf005667b263e0e8a1ccfb8daec.</p>
Strike HZ_6cc83804	<p>This strike sends a malware sample known as HZ. HZ is Remote Access Trojan backdoor. This is a macOS version of HZ that was has been associated with popular messaging apps like DingTalk and WeChat. The malware collects the victim information and communicates with a C2 server to execute additional commands. The MD5 hash of this HZ sample is 6cc838049ece4fcb36386b7a3032171f.</p>
Strike HZ_6d478c7f	<p>This strike sends a malware sample known as HZ. HZ is Remote Access Trojan backdoor. This is a macOS version of HZ that was has been associated with popular messaging apps like DingTalk and WeChat. The malware collects the victim information and communicates with a C2 server to execute additional commands. The MD5 hash of this HZ sample is 6d478c7f94d95981eb4b6508844050a6.</p>

<b>Name</b>	<b>Description</b>
Strike HZ_7005c9c6	This strike sends a malware sample known as HZ. HZ is Remote Access Trojan backdoor. This is a macOS version of HZ that was has been associated with popular messaging apps like DingTalk and WeChat. The malware collects the victim information and communicates with a C2 server to execute additional commands. The MD5 hash of this HZ sample is 7005c9c6e2502992017f1ffc8ef8a9b9.
Strike HZ_7355e079	This strike sends a malware sample known as HZ. HZ is Remote Access Trojan backdoor. This is a macOS version of HZ that was has been associated with popular messaging apps like DingTalk and WeChat. The malware collects the victim information and communicates with a C2 server to execute additional commands. The MD5 hash of this HZ sample is 7355e0790c111a59af377babedee9018.
Strike HZ_7a66cd84	This strike sends a malware sample known as HZ. HZ is Remote Access Trojan backdoor. This is a macOS version of HZ that was has been associated with popular messaging apps like DingTalk and WeChat. The malware collects the victim information and communicates with a C2 server to execute additional commands. The MD5 hash of this HZ sample is 7a66cd84e2d007664a66679e86832202.
Strike HZ_7ed3fc83	This strike sends a malware sample known as HZ. HZ is Remote Access Trojan backdoor. This is a macOS version of HZ that was has been associated with popular messaging apps like DingTalk and WeChat. The malware collects the victim information and communicates with a C2 server to execute additional commands. The MD5 hash of this HZ sample is 7ed3fc831922733d70fb08da7a244224.
Strike HZ_9cdb61a7	This strike sends a malware sample known as HZ. HZ is Remote Access Trojan backdoor. This is a macOS version of HZ that was has been associated with popular messaging apps like DingTalk and WeChat. The malware collects the victim information and communicates with a C2 server to execute additional commands. The MD5 hash of this HZ sample is 9cdb61a758afd9a893add4cef5608914.
Strike HZ_da07b060	This strike sends a malware sample known as HZ. HZ is Remote Access Trojan backdoor. This is a macOS version of HZ that was has been associated with popular messaging apps like DingTalk and WeChat. The malware collects the victim information and communicates with a C2 server to execute additional commands. The MD5 hash of this HZ sample is da07b0608195a2d5481ad6de3cc6f195.
Strike HZ_dd71b279	This strike sends a malware sample known as HZ. HZ is Remote Access Trojan backdoor. This is a macOS version of HZ that was has been associated with popular messaging apps like DingTalk and WeChat. The malware collects the victim information and communicates with a C2 server to execute additional commands. The MD5 hash of this HZ sample is dd71b279a0bf618bbe9bb5d934ce9caa.
Strike Hades_9fa1ba3e	This strike sends a malware sample known as Hades. Hades is a ransomware created by the cyber-criminal group INDRIK SPIDER, also known as Evil Corp. It shares most of its functionality with WastedLocker and is thus considered a derivative of it. The MD5 hash of this Hades sample is 9fa1ba3e7d6e32f240c790753cdaf8e.

<b>Name</b>	<b>Description</b>
Strike Haron_04ef9ed3	This strike sends a malware sample known as Haron. Haron is a ransomware that is being considered a copy or derivative of the Avaddon and Thanos ransomware. It uses the Thanos framework to infect victims, which was made open source, and the Avaddon UI which was also leaked. The MD5 hash of this Haron sample is 04ef9ed3902dadccabb678c9dad53f19.
Strike Haron_27757047	This strike sends a malware sample known as Haron. Haron is a ransomware that is being considered a copy or derivative of the Avaddon and Thanos ransomware. It uses the Thanos framework to infect victims, which was made open source, and the Avaddon UI which was also leaked. The MD5 hash of this Haron sample is 277570474740f06232e009b5ff15d47a.
Strike Haron_6da3c779	This strike sends a malware sample known as Haron. Haron is a ransomware that is being considered a copy or derivative of the Avaddon and Thanos ransomware. It uses the Thanos framework to infect victims, which was made open source, and the Avaddon UI which was also leaked. The MD5 hash of this Haron sample is 6da3c7796bca2f47f11e8711a945cf1d.
Strike Haron_731797d3	This strike sends a malware sample known as Haron. Haron is a ransomware that is being considered a copy or derivative of the Avaddon and Thanos ransomware. It uses the Thanos framework to infect victims, which was made open source, and the Avaddon UI which was also leaked. The MD5 hash of this Haron sample is 731797d30d8ff6eaf901e788bd4e6048.
Strike Haron_7806efea	This strike sends a polymorphic malware sample known as Haron. Haron is a ransomware that is being considered a copy or derivative of the Avaddon and Thanos ransomware. It uses the Thanos framework to infect victims, which was made open source, and the Avaddon UI which was also leaked. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Haron sample is 7806efea649a3b312be91e609541359b.
Strike Haron_92c2e2f6	This strike sends a polymorphic malware sample known as Haron. Haron is a ransomware that is being considered a copy or derivative of the Avaddon and Thanos ransomware. It uses the Thanos framework to infect victims, which was made open source, and the Avaddon UI which was also leaked. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Haron sample is 92c2e2f66b9717304aa67c9114b959c2.
Strike Haron_af79a121	This strike sends a malware sample known as Haron. Haron is a ransomware that is being considered a copy or derivative of the Avaddon and Thanos ransomware. It uses the Thanos framework to infect victims, which was made open source, and the Avaddon UI which was also leaked. The MD5 hash of this Haron sample is af79a121a5c315f5a7b8a2180ccbea0f.
Strike Haron_dedad693	This strike sends a malware sample known as Haron. Haron is a ransomware that is being considered a copy or derivative of the Avaddon and Thanos ransomware. It uses the Thanos framework to infect victims, which was made open source, and the Avaddon UI which was also leaked. The MD5 hash of this Haron sample is dedad693898bba0e4964e6c9a749d380.

<b>Name</b>	<b>Description</b>
Strike Haron_e8f8e4eb	This strike sends a malware sample known as Haron. Haron is a ransomware that is being considered a copy or derivative of the Avaddon and Thanos ransomware. It uses the Thanos framework to infect victims, which was made open source, and the Avaddon UI which was also leaked. The MD5 hash of this Haron sample is e8f8e4eb0d2c03f0b12fb1cf09932bbd.
Strike HawkEye_2a759d9c	This strike sends a malware sample known as HawkEye. HawkEye is an information stealing malware that specifically targets usernames and passwords stored by web browsers and mail clients on an infected machine. It is commonly spread via email and can also propagate through removable media. The MD5 hash of this HawkEye sample is 2a759d9cc498a190f3f8c71f57e65644.
Strike HawkEye_3ba7171c	This strike sends a malware sample known as HawkEye. HawkEye is an information stealing malware that specifically targets usernames and passwords stored by web browsers and mail clients on an infected machine. It is commonly spread via email and can also propagate through removable media. The MD5 hash of this HawkEye sample is 3ba7171c8836de935a74799291ebca46.
Strike HawkEye_3eb89430	This strike sends a malware sample known as HawkEye. HawkEye is an information stealing malware that specifically targets usernames and passwords stored by web browsers and mail clients on an infected machine. It is commonly spread via email and can also propagate through removable media. The MD5 hash of this HawkEye sample is 3eb89430ad1c97dc03a85175299a5a37.
Strike HawkEye_600fb168	This strike sends a malware sample known as HawkEye. HawkEye is an information stealing malware that specifically targets usernames and passwords stored by web browsers and mail clients on an infected machine. It is commonly spread via email and can also propagate through removable media. The MD5 hash of this HawkEye sample is 600fb1681d639f913b70884da6996d5a.
Strike HawkEye_65e73f93	This strike sends a malware sample known as HawkEye. HawkEye is an information stealing malware that specifically targets usernames and passwords stored by web browsers and mail clients on an infected machine. It is commonly spread via email and can also propagate through removable media. The MD5 hash of this HawkEye sample is 65e73f938774b6dfadea69ac7cb37193.
Strike HawkEye_88b882aa	This strike sends a malware sample known as HawkEye. HawkEye is an information stealing malware that specifically targets usernames and passwords stored by web browsers and mail clients on an infected machine. It is commonly spread via email and can also propagate through removable media. The MD5 hash of this HawkEye sample is 88b882aacd9a1ca0f1f7304c21aaae66.
Strike HawkEye_9ea93fd1	This strike sends a malware sample known as HawkEye. HawkEye is an information stealing malware that specifically targets usernames and passwords stored by web browsers and mail clients on an infected machine. It is commonly spread via email and can also propagate through removable media. The MD5 hash of this HawkEye sample is 9ea93fd1175bb07b354c496ee3a04664.
Strike HawkEye_a818e1ed	This strike sends a malware sample known as HawkEye. HawkEye is an information stealing malware that specifically targets usernames and passwords stored by web browsers and mail clients on an infected machine. It is commonly spread via email and can also propagate through removable media. The MD5 hash of this HawkEye sample is a818e1ed86f7fa07ac47954694bc91fe.

<b>Name</b>	<b>Description</b>
Strike HawkEye_bc66e2a1	This strike sends a malware sample known as HawkEye. HawkEye is an information stealing malware that specifically targets usernames and passwords stored by web browsers and mail clients on an infected machine. It is commonly spread via email and can also propagate through removable media. The MD5 hash of this HawkEye sample is bc66e2a191d06f12b1a035975660052b.
Strike HawkEye_bd568bca	This strike sends a malware sample known as HawkEye. HawkEye is an information stealing malware that specifically targets usernames and passwords stored by web browsers and mail clients on an infected machine. It is commonly spread via email and can also propagate through removable media. The MD5 hash of this HawkEye sample is bd568bcacc3b34646de7676d03ff741e.
Strike HawkEye_ed31cc34	This strike sends a malware sample known as HawkEye. HawkEye is an information stealing malware that specifically targets usernames and passwords stored by web browsers and mail clients on an infected machine. It is commonly spread via email and can also propagate through removable media. The MD5 hash of this HawkEye sample is ed31cc349fffdc64e35ad4b149c06d55.
Strike HawkEye_f0d75fb8	This strike sends a malware sample known as HawkEye. HawkEye is an information stealing malware that specifically targets usernames and passwords stored by web browsers and mail clients on an infected machine. It is commonly spread via email and can also propagate through removable media. The MD5 hash of this HawkEye sample is f0d75fb839b44dc8d064b7bf8295f94d.
Strike HawkEye_f4274360	This strike sends a malware sample known as HawkEye. HawkEye is an information stealing malware that specifically targets usernames and passwords stored by web browsers and mail clients on an infected machine. It is commonly spread via email and can also propagate through removable media. The MD5 hash of this HawkEye sample is f4274360fefd50fb219f0ec648bf015e.
Strike HawkEye_f5968828	This strike sends a malware sample known as HawkEye. HawkEye is an information stealing malware that specifically targets usernames and passwords stored by web browsers and mail clients on an infected machine. It is commonly spread via email and can also propagate through removable media. The MD5 hash of this HawkEye sample is f59688280c0e7c9122ba24ae6c1274b9.
Strike HermeticWiper_14f42b51	This strike sends a polymorphic malware sample known as HermeticWiper. In February 2022 a new wave of wiper attacks against the country of Ukraine was detected. The malware HermeticWiper exhibits similar functionality to the previous wiper malware WhisperGate used in cyber attacks against Ukraine. Like WhisperGate this wiper malware will target the Master Boot Record and attempt to destroy it. It also includes a component that will enumerate the system partitions and wipe all files on the targeted system. The binary has the debug flag removed in the PE file format. The MD5 hash of this HermeticWiper sample is 14f42b516044fc2db11745ad9c557ed9.
Strike HermeticWiper_3f4a16b2	This strike sends a malware sample known as HermeticWiper. In February 2022 a new wave of wiper attacks against the country of Ukraine was detected. The malware HermeticWiper exhibits similar functionality to the previous wiper malware WhisperGate used in cyber attacks against Ukraine. Like WhisperGate this wiper malware will target the Master Boot Record and attempt to destroy it. It also includes a component that will enumerate the system partitions and wipe all files on the targeted system. The MD5 hash of this HermeticWiper sample is 3f4a16b29f2f0532b7ce3e7656799125.

<b>Name</b>	<b>Description</b>
Strike HermeticWiper_4b1f04cf	This strike sends a polymorphic malware sample known as HermeticWiper. In February 2022 a new wave of wiper attacks against the country of Ukraine was detected. The malware HermeticWiper exhibits similar functionality to the previous wiper malware WhisperGate used in cyber attacks against Ukraine. Like WhisperGate this wiper malware will target the Master Boot Record and attempt to destroy it. It also includes a component that will enumerate the system partitions and wipe all files on the targeted system. The binary has the timestamp field updated in the PE file header. The MD5 hash of this HermeticWiper sample is 4b1f04cf967a73c4ce1e3ab3c492805e.
Strike HermeticWiper_5d693a27	This strike sends a polymorphic malware sample known as HermeticWiper. In February 2022 a new wave of wiper attacks against the country of Ukraine was detected. The malware HermeticWiper exhibits similar functionality to the previous wiper malware WhisperGate used in cyber attacks against Ukraine. Like WhisperGate this wiper malware will target the Master Boot Record and attempt to destroy it. It also includes a component that will enumerate the system partitions and wipe all files on the targeted system. The binary has random bytes appended at the end of the file. The MD5 hash of this HermeticWiper sample is 5d693a277a0cd4ff86f2b43b193f8315.
Strike HermeticWiper_84ba0197	This strike sends a malware sample known as HermeticWiper. In February 2022 a new wave of wiper attacks against the country of Ukraine was detected. The malware HermeticWiper exhibits similar functionality to the previous wiper malware WhisperGate used in cyber attacks against Ukraine. Like WhisperGate this wiper malware will target the Master Boot Record and attempt to destroy it. It also includes a component that will enumerate the system partitions and wipe all files on the targeted system. The MD5 hash of this HermeticWiper sample is 84ba0197920fd3e2b7dfa719fee09d2f.
Strike HermeticWiper_9bc9babd	This strike sends a polymorphic malware sample known as HermeticWiper. In February 2022 a new wave of wiper attacks against the country of Ukraine was detected. The malware HermeticWiper exhibits similar functionality to the previous wiper malware WhisperGate used in cyber attacks against Ukraine. Like WhisperGate this wiper malware will target the Master Boot Record and attempt to destroy it. It also includes a component that will enumerate the system partitions and wipe all files on the targeted system. The binary has the checksum removed in the PE file format. The MD5 hash of this HermeticWiper sample is 9bc9babd952fb816609e3031f8c136e3.
Strike HermeticWiper_a70b4e3e	This strike sends a polymorphic malware sample known as HermeticWiper. In February 2022 a new wave of wiper attacks against the country of Ukraine was detected. The malware HermeticWiper exhibits similar functionality to the previous wiper malware WhisperGate used in cyber attacks against Ukraine. Like WhisperGate this wiper malware will target the Master Boot Record and attempt to destroy it. It also includes a component that will enumerate the system partitions and wipe all files on the targeted system. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this HermeticWiper sample is a70b4e3e88f3fcc48b7ee8426aa8833e.

<b>Name</b>	<b>Description</b>
Strike HermeticWiper_aa86953f	This strike sends a polymorphic malware sample known as HermeticWiper. In February 2022 a new wave of wiper attacks against the country of Ukraine was detected. The malware HermeticWiper exhibits similar functionality to the previous wiper malware WhisperGate used in cyber attacks against Ukraine. Like WhisperGate this wiper malware will target the Master Boot Record and attempt to destroy it. It also includes a component that will enumerate the system partitions and wipe all files on the targeted system. The binary has the debug flag removed in the PE file format. The MD5 hash of this HermeticWiper sample is aa86953f2915b113252c5c0a937329b4.
Strike HermeticWiper_baa339df	This strike sends a polymorphic malware sample known as HermeticWiper. In February 2022 a new wave of wiper attacks against the country of Ukraine was detected. The malware HermeticWiper exhibits similar functionality to the previous wiper malware WhisperGate used in cyber attacks against Ukraine. Like WhisperGate this wiper malware will target the Master Boot Record and attempt to destroy it. It also includes a component that will enumerate the system partitions and wipe all files on the targeted system. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this HermeticWiper sample is baa339dfc70bd3094bed69f773db5338.
Strike HermeticWiper_bc0c5e0c	This strike sends a polymorphic malware sample known as HermeticWiper. In February 2022 a new wave of wiper attacks against the country of Ukraine was detected. The malware HermeticWiper exhibits similar functionality to the previous wiper malware WhisperGate used in cyber attacks against Ukraine. Like WhisperGate this wiper malware will target the Master Boot Record and attempt to destroy it. It also includes a component that will enumerate the system partitions and wipe all files on the targeted system. The binary has the checksum removed in the PE file format. The MD5 hash of this HermeticWiper sample is bc0c5e0c68b810559f552827f80b81c2.
Strike HermeticWiper_c7eb0c34	This strike sends a polymorphic malware sample known as HermeticWiper. In February 2022 a new wave of wiper attacks against the country of Ukraine was detected. The malware HermeticWiper exhibits similar functionality to the previous wiper malware WhisperGate used in cyber attacks against Ukraine. Like WhisperGate this wiper malware will target the Master Boot Record and attempt to destroy it. It also includes a component that will enumerate the system partitions and wipe all files on the targeted system. The binary has been packed using upx packer, with the default options. The MD5 hash of this HermeticWiper sample is c7eb0c341441550dd0743e6a992c4c3f.
Strike HermeticWiper_e19137f2	This strike sends a polymorphic malware sample known as HermeticWiper. In February 2022 a new wave of wiper attacks against the country of Ukraine was detected. The malware HermeticWiper exhibits similar functionality to the previous wiper malware WhisperGate used in cyber attacks against Ukraine. Like WhisperGate this wiper malware will target the Master Boot Record and attempt to destroy it. It also includes a component that will enumerate the system partitions and wipe all files on the targeted system. The binary has random bytes appended at the end of the file. The MD5 hash of this HermeticWiper sample is e19137f2f707150493887c1504c3a794.

<b>Name</b>	<b>Description</b>
Strike HermeticWiper_ece4f943	This strike sends a polymorphic malware sample known as HermeticWiper. In February 2022 a new wave of wiper attacks against the country of Ukraine was detected. The malware HermeticWiper exhibits similar functionality to the previous wiper malware WhisperGate used in cyber attacks against Ukraine. Like WhisperGate this wiper malware will target the Master Boot Record and attempt to destroy it. It also includes a component that will enumerate the system partitions and wipe all files on the targeted system. The binary has the timestamp field updated in the PE file header. The MD5 hash of this HermeticWiper sample is ece4f943b6d5d11ff42b071fe775922e.
Strike HermeticWiper_fdfbd04e	This strike sends a polymorphic malware sample known as HermeticWiper. In February 2022 a new wave of wiper attacks against the country of Ukraine was detected. The malware HermeticWiper exhibits similar functionality to the previous wiper malware WhisperGate used in cyber attacks against Ukraine. Like WhisperGate this wiper malware will target the Master Boot Record and attempt to destroy it. It also includes a component that will enumerate the system partitions and wipe all files on the targeted system. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this HermeticWiper sample is fdfbd04e7ff74c3cddc315f739f241ff.
Strike HijackLoader_0f3a6907	This strike sends a malware sample known as HijackLoader. HijackLoader is a malware loader. It has been associated with many malware families like Danabot, SystemBC, and RedLine Stealer. The MD5 hash of this HijackLoader sample is 0f3a69075e511390b5fdb4687f47ea0b.
Strike HijackLoader_202778ea	This strike sends a malware sample known as HijackLoader. HijackLoader is a malware loader. It has been associated with many malware families like Danabot, SystemBC, and RedLine Stealer. The MD5 hash of this HijackLoader sample is 202778ea30aea10369819e0856be68cd.
Strike HijackLoader_90454b28	This strike sends a malware sample known as HijackLoader. HijackLoader is a malware loader. It has been associated with many malware families like Danabot, SystemBC, and RedLine Stealer. The MD5 hash of this HijackLoader sample is 90454b28a84ef4460cebb209f4f32a9f.
Strike HijackLoader_93a03e99	This strike sends a malware sample known as HijackLoader. HijackLoader is a malware loader. It has been associated with many malware families like Danabot, SystemBC, and RedLine Stealer. The MD5 hash of this HijackLoader sample is 93a03e997a9654d4fd303da4af077a82.
Strike HijackLoader_de9002d3	This strike sends a malware sample known as HijackLoader. HijackLoader is a malware loader. It has been associated with many malware families like Danabot, SystemBC, and RedLine Stealer. The MD5 hash of this HijackLoader sample is de9002d3048e6500b767fe8a98ef5cd9.
Strike Hive_036539c8	This strike sends a malware sample known as Hive. Hive is a popular Ransomware as a Service malware written in Go and Rust. This malware has been used in attacks in both the healthcare and software industries. The ransomware encrypts all data on the system and informs the victim that their personal data will be exfiltrated and disclosed unless the ransom is paid. The MD5 hash of this Hive sample is 036539c87a839b419424c8d535252185.

<b>Name</b>	<b>Description</b>
Strike Hive_0f3e5603	This strike sends a malware sample known as Hive. Hive is a popular Ransomware as a Service malware written in Go and Rust. This malware has been used in attacks in both the healthcare and software industries. The ransomware encrypts all data on the system and informs the victim that their personal data will be exfiltrated and disclosed unless the ransom is paid. The MD5 hash of this Hive sample is 0f3e5603cf3f5cc91e8eb031a4b5c45d.
Strike Hive_2c3d2910	This strike sends a malware sample known as Hive. Hive is a popular Ransomware as a Service malware written in Go and Rust. This malware has been used in attacks in both the healthcare and software industries. The ransomware encrypts all data on the system and informs the victim that their personal data will be exfiltrated and disclosed unless the ransom is paid. The MD5 hash of this Hive sample is 2c3d2910e6e4a6b739b4253fc当地34e2。
Strike Hive_2eafe1d0	This strike sends a malware sample known as Hive. Hive is a popular Ransomware as a Service malware written in Go and Rust. This malware has been used in attacks in both the healthcare and software industries. The ransomware encrypts all data on the system and informs the victim that their personal data will be exfiltrated and disclosed unless the ransom is paid. The MD5 hash of this Hive sample is 2eafe1d0f2579e730ed03445bff12d0c。
Strike Hive_4144a0d0	This strike sends a malware sample known as Hive. Hive is a popular Ransomware as a Service malware written in Go and Rust. This malware has been used in attacks in both the healthcare and software industries. The ransomware encrypts all data on the system and informs the victim that their personal data will be exfiltrated and disclosed unless the ransom is paid. The MD5 hash of this Hive sample is 4144a0d0777073b1c5d83d743682c5e9。
Strike Hive_6d531ec9	This strike sends a malware sample known as Hive. Hive is a popular Ransomware as a Service malware written in Go and Rust. This malware has been used in attacks in both the healthcare and software industries. The ransomware encrypts all data on the system and informs the victim that their personal data will be exfiltrated and disclosed unless the ransom is paid. The MD5 hash of this Hive sample is 6d531ec923346d7d29b7aa8fe7df2c94。
Strike Hive_700ab60c	This strike sends a malware sample known as Hive. Hive is a popular Ransomware as a Service malware written in Go and Rust. This malware has been used in attacks in both the healthcare and software industries. The ransomware encrypts all data on the system and informs the victim that their personal data will be exfiltrated and disclosed unless the ransom is paid. The MD5 hash of this Hive sample is 700ab60cd8ea41c959394479d0baf5e。
Strike Hive_d7fb1939	This strike sends a malware sample known as Hive. Hive is a popular Ransomware as a Service malware written in Go and Rust. This malware has been used in attacks in both the healthcare and software industries. The ransomware encrypts all data on the system and informs the victim that their personal data will be exfiltrated and disclosed unless the ransom is paid. The MD5 hash of this Hive sample is d7fb1939cf5bda2d2c6b792324554dfc。

<b>Name</b>	<b>Description</b>
Strike HomeLand Justice Encryptor_11e534e8	This strike sends a polymorphic malware sample known as HomeLand Justice Encryptor. Iranian state cyber actors calling themselves "HomeLand Justice" launched a cyber attack against the Government of Albania. During the attack the attackers conducted lateral movements, network reconnaissance, and credential harvesting against the Albanian Government. This attack also included a ransomware-style file encryptor and disk wiping malware. This sample is the GoXML.exe ransomware encryptor. The binary has random bytes appended at the end of the file. The MD5 hash of this HomeLand Justice Encryptor sample is 11e534e8f9f6d2068a97d07e6b2e95d4.
Strike HomeLand Justice Encryptor_2e3f4d0c	This strike sends a polymorphic malware sample known as HomeLand Justice Encryptor. Iranian state cyber actors calling themselves "HomeLand Justice" launched a cyber attack against the Government of Albania. During the attack the attackers conducted lateral movements, network reconnaissance, and credential harvesting against the Albanian Government. This attack also included a ransomware-style file encryptor and disk wiping malware. This sample is the GoXML.exe ransomware encryptor. The binary has the checksum removed in the PE file format. The MD5 hash of this HomeLand Justice Encryptor sample is 2e3f4d0c18c040e8ff0b8d8da1cbcc84.
Strike HomeLand Justice Encryptor_2fc18ad9	This strike sends a polymorphic malware sample known as HomeLand Justice Encryptor. Iranian state cyber actors calling themselves "HomeLand Justice" launched a cyber attack against the Government of Albania. During the attack the attackers conducted lateral movements, network reconnaissance, and credential harvesting against the Albanian Government. This attack also included a ransomware-style file encryptor and disk wiping malware. This sample is the GoXML.exe ransomware encryptor. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this HomeLand Justice Encryptor sample is 2fc18ad9d19c40895dfa3aa743188082.
Strike HomeLand Justice Encryptor_369ddb9e	This strike sends a polymorphic malware sample known as HomeLand Justice Encryptor. Iranian state cyber actors calling themselves "HomeLand Justice" launched a cyber attack against the Government of Albania. During the attack the attackers conducted lateral movements, network reconnaissance, and credential harvesting against the Albanian Government. This attack also included a ransomware-style file encryptor and disk wiping malware. This sample is the GoXML.exe ransomware encryptor. The binary has the timestamp field updated in the PE file header. The MD5 hash of this HomeLand Justice Encryptor sample is 369ddb9e0d94793f0f70dfa3d8d2079f.
Strike HomeLand Justice Encryptor_64035692	This strike sends a polymorphic malware sample known as HomeLand Justice Encryptor. Iranian state cyber actors calling themselves "HomeLand Justice" launched a cyber attack against the Government of Albania. During the attack the attackers conducted lateral movements, network reconnaissance, and credential harvesting against the Albanian Government. This attack also included a ransomware-style file encryptor and disk wiping malware. This sample is the GoXML.exe ransomware encryptor. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this HomeLand Justice Encryptor sample is 64035692b7c55caf9fd4d2535a5face3.

<b>Name</b>	<b>Description</b>
Strike HomeLand Justice Encryptor_9adc34da	This strike sends a polymorphic malware sample known as HomeLand Justice Encryptor. Iranian state cyber actors calling themselves "HomeLand Justice" launched a cyber attack against the Government of Albania. During the attack the attackers conducted lateral movements, network reconnaissance, and credential harvesting against the Albanian Government. This attack also included a ransomware-style file encryptor and disk wiping malware. This sample is the GoXML.exe ransomware encryptor. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this HomeLand Justice Encryptor sample is 9adc34da79436d216d6c19f992196f6b.
Strike HomeLand Justice Encryptor_bbe983db	This strike sends a malware sample known as HomeLand Justice Encryptor. Iranian state cyber actors calling themselves "HomeLand Justice" launched a cyber attack against the Government of Albania. During the attack the attackers conducted lateral movements, network reconnaissance, and credential harvesting against the Albanian Government. This attack also included a ransomware-style file encryptor and disk wiping malware. This sample is the GoXML.exe ransomware encryptor. The MD5 hash of this HomeLand Justice Encryptor sample is bbe983dba3bf319621b447618548b740.
Strike HomeLand Justice Wiper_7b717642	This strike sends a malware sample known as HomeLand Justice Wiper. Iranian state cyber actors calling themselves "HomeLand Justice" launched a cyber attack against the Government of Albania. During the attack the attackers conducted lateral movements, network reconnaissance, and credential harvesting against the Albanian Government. This attack also included a ransomware-style file encryptor and disk wiping malware. This sample is the disk wiper. The MD5 hash of this HomeLand Justice Wiper sample is 7b71764236f244ae971742ee1bc6b098.
Strike Hook_21d8304c	This strike sends a malware sample known as Hook. Hook is an Android RAT malware variant based off of the Ermac malware. Hook has the capability to manipulate files on the device as well as interact with the System's UI. This includes the ability to perform gestures, take screenshots, simulate clicks and keypresses, unlocking the device, scrolling, and clicking ui text elements. The MD5 hash of this Hook sample is 21d8304cb6e169db00d6f19d346e4152.
Strike Hook_54d7ec1e	This strike sends a malware sample known as Hook. Hook is an Android RAT malware variant based off of the Ermac malware. Hook has the capability to manipulate files on the device as well as interact with the System's UI. This includes the ability to perform gestures, take screenshots, simulate clicks and keypresses, unlocking the device, scrolling, and clicking ui text elements. The MD5 hash of this Hook sample is 54d7ec1e7d5f8f2884281cdafabae3c0.
Strike Hook_6e886c71	This strike sends a malware sample known as Hook. Hook is an Android RAT malware variant based off of the Ermac malware. Hook has the capability to manipulate files on the device as well as interact with the System's UI. This includes the ability to perform gestures, take screenshots, simulate clicks and keypresses, unlocking the device, scrolling, and clicking ui text elements. The MD5 hash of this Hook sample is 6e886c71b9663012f6659f347790c979.

<b>Name</b>	<b>Description</b>
Strike Hook_8e6116cc	This strike sends a malware sample known as Hook. Hook is an Android RAT malware variant based off of the Ermac malware. Hook has the capability to manipulate files on the device as well as interact with the System's UI. This includes the ability to perform gestures, take screenshots, simulate clicks and keypresses, unlocking the device, scrolling, and clicking ui text elements. The MD5 hash of this Hook sample is 8e6116cc7b74c87520a340c4de6dd911.
Strike HorusAgent_00c05d72	This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is 00c05d72920d62077b7c670919214339.
Strike HorusAgent_04409d6f	This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is 04409d6fb02c66e4a928c5c7bf1cf663.
Strike HorusAgent_316f9713	This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is 316f9713641f03e13cc0ee2fae244e48.
Strike HorusAgent_3ef3ac25	This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is 3ef3ac25c48c8a1daa74c01b5f695cfb.

<b>Name</b>	<b>Description</b>
Strike HorusAgent_5cd9a21c	<p>This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is 5cd9a21ca2d496210caf3ce8362c309b.</p>
Strike HorusAgent_64f47ce2	<p>This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is 64f47ce2f7528b48c6cc9cddc1f48fa3.</p>
Strike HorusAgent_70c93643	<p>This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is 70c93643ff5171a362e05f41306f0c16.</p>
Strike HorusAgent_71b625f0	<p>This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is 71b625f00d53987303b6d23e0bbcbd0a.</p>

<b>Name</b>	<b>Description</b>
Strike HorusAgent_88c47fc4	<p>This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is 88c47fc4a84adbcfada7d8ea98790252.</p>
Strike HorusAgent_9dd15d21	<p>This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is 9dd15d21ff456e525ef4fba26eaedc0d.</p>
Strike HorusAgent_a17d21ba	<p>This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is a17d21baa4329d6affb6f0436efc3ce2.</p>
Strike HorusAgent_b05dc7c8	<p>This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is b05dc7c8dba865cccd3169df3dd3aab45.</p>

Name	Description
Strike HorusAgent_cdc23eb5	<p>This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is cdc23eb5187ae4ca82859fb818e5c3eb.</p>
Strike HorusAgent_e9ccd7e8	<p>This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is e9ccd7e8db309e146445e364f48b9068.</p>
Strike HorusAgent_ead247b9	<p>This strike sends a malware sample known as Horus Agent. This strike sends a malware sample known as Horus Agent. Horus Agent is part of a cyberespionage campaign conducted by the Stealth Falcon threat group. It is delivered through a malicious .url file disguised as a PDF that exploits CVE 2025 33053, a zero day vulnerability in Windows WebDAV, to execute payloads via iediagcmd.exe. The malware chain includes Horus Loader, which uses evasion techniques like anti-VM checks and DLL mapping, and deploys Horus Agent, a C++ implant based on the Mythic C2 framework. The agent supports remote access, shellcode injection, file operations, and includes modules for credential theft and keylogging. The MD5 hash of this Horus Agent sample is ead247b90ebd4aad7a4cf29f0e4eb111.</p>
Strike Hupigon_05fa4098	<p>This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 05fa4098d6102c38982ed2bb55ac21d6.</p>
Strike Hupigon_06f83b6c	<p>This strike sends a polymorphic malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Hupigon sample is 06f83b6c4f704afffe9d48727720416a.</p>
Strike Hupigon_07c75bae	<p>This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 07c75baee5a6ae81ac978acba8a3d8aa.</p>

<b>Name</b>	<b>Description</b>
Strike Hupigon_1600de31	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 1600de312560e6b773d382413aa70e74.
Strike Hupigon_1a979031	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 1a9790316f17c8a39dd67772f78ba2bd.
Strike Hupigon_1e9bbb20	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 1e9bbb205b4c79024fcc440bd1130726.
Strike Hupigon_1f9f5ce9	This strike sends a polymorphic malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The binary has been packed using upx packer, with the default options. The MD5 hash of this Hupigon sample is 1f9f5ce911834cf72f799844da29d977.
Strike Hupigon_20517e6b	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 20517e6b94106686ef81d375c90c2022.
Strike Hupigon_227154fb	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 227154fb5f024c0d8a0be9b0df612ea3.
Strike Hupigon_2b20a40b	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 2b20a40beb5838ae90e96d1ae9d25283.
Strike Hupigon_2b6f5cd3	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 2b6f5cd3688abd349f4cfb94164562cb.
Strike Hupigon_2da2d409	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 2da2d4091b9ad9050d9f2127e69f56b0.

<b>Name</b>	<b>Description</b>
Strike Hupigon_339275e0	This strike sends a polymorphic malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Hupigon sample is 339275e0728bc68486e1862bae27b0b6.
Strike Hupigon_3d4a8ff6	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 3d4a8ff63982abce0518079deb731a83.
Strike Hupigon_3eb62f14	This strike sends a polymorphic malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The binary has random bytes appended at the end of the file. The MD5 hash of this Hupigon sample is 3eb62f14ed0821f7b9b366c83f3dcad1.
Strike Hupigon_43b43e55	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 43b43e552fdb6948382c4f7bd8c80017.
Strike Hupigon_4c37493e	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 4c37493e8bd5bd0e734e252aa0be12e5.
Strike Hupigon_5096942b	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 5096942b5ae645047759f038bde79ee2.
Strike Hupigon_51e34a25	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 51e34a25e65889cf833ec220329c487c.
Strike Hupigon_53b1c580	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 53b1c580939176a264a724ba4c2493bc.
Strike Hupigon_57ae6c60	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 57ae6c6014102b320c80edcc1f385366.
Strike Hupigon_58303826	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 58303826aae3c74a9465e4df449426ad.

<b>Name</b>	<b>Description</b>
Strike Hupigon_5e15f278	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 5e15f2784f98d21c45029623610e268a.
Strike Hupigon_5e185489	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 5e18548913107bd5506a21bd541b25ae.
Strike Hupigon_5ed9157b	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 5ed9157b529b233195ba77a6c0f60807.
Strike Hupigon_660a2d53	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 660a2d53655c5ff3c1fc1852095c1624.
Strike Hupigon_689678d7	This strike sends a polymorphic malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Hupigon sample is 689678d733098faf9138197421f1b25.
Strike Hupigon_743e0997	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 743e0997dae362f311869bb9f4fa5abc.
Strike Hupigon_787230e2	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 787230e27a9cd49f59429a8b86636877.
Strike Hupigon_78860c61	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 78860c61167bb648a081ab7371638247.
Strike Hupigon_7937c41d	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 7937c41d346e489bbe34bc996fc11455.
Strike Hupigon_793c7c56	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 793c7c568ef53df8d3e838c1119b509e.

<b>Name</b>	<b>Description</b>
Strike Hupigon_8d7a6e0a	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 8d7a6e0a188f39c414d6b8e40880a9cf.
Strike Hupigon_90468611	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 90468611aba2c7267ab82b46b69eb413.
Strike Hupigon_964bd073	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 964bd07332952fe78d3cdc44a20e64d7.
Strike Hupigon_9c25b770	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 9c25b77077f44d79fc5366eb54b22bbd.
Strike Hupigon_9d00848b	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is 9d00848b8978a0fd33214b78662f90c1.
Strike Hupigon_9efb0665	This strike sends a polymorphic malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Hupigon sample is 9efb06656eabd91cf27272343e11f014.
Strike Hupigon_a43dd785	This strike sends a polymorphic malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The binary has the checksum removed in the PE file format. The MD5 hash of this Hupigon sample is a43dd7859c056269b1de939f77e7136b.
Strike Hupigon_a52d0b02	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is a52d0b02fc623f4d0ada0e5c5432c559.
Strike Hupigon_a8e0c1a2	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is a8e0c1a24ef3690eb2c8c79ea8fc880a.

<b>Name</b>	<b>Description</b>
Strike Hupigon_a94f8d04	This strike sends a polymorphic malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The binary has been packed using upx packer, with the default options. The MD5 hash of this Hupigon sample is a94f8d044abf12e2bd92184ad1e7fa22.
Strike Hupigon_aeab478c	This strike sends a polymorphic malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Hupigon sample is aeab478c4e5be8e682730d61ff01ac6e.
Strike Hupigon_b17a8e87	This strike sends a polymorphic malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The binary has random bytes appended at the end of the file. The MD5 hash of this Hupigon sample is b17a8e87539667748cd74b4c4da8aea9.
Strike Hupigon_b5f51c06	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is b5f51c06af27f4f20d9e30b2fd7bc809.
Strike Hupigon_b6f5353f	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is b6f5353f224817d241ef24fdf594b22c.
Strike Hupigon_b8776276	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is b8776276dcd39631753cac978f8ec9a1.
Strike Hupigon_b8aec15b	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is b8aec15bb1d5f7690685c735fb285483.
Strike Hupigon_bbdd2e9e	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is bbdd2e9e288862a2e2048871ec43a398.
Strike Hupigon_bceef9b5	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is bceef9b557f482e6395108967b42e159.

<b>Name</b>	<b>Description</b>
Strike Hupigon_be41beee	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is be41beee7e99e2a6fc79bd6bc0032b59.
Strike Hupigon_d31fd664	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is d31fd6646d114a6c8b41772f82e3e38b.
Strike Hupigon_d6a6b2f9	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is d6a6b2f9bd1a53e3789bcf5b4865aa81.
Strike Hupigon_d8b33080	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is d8b33080023b54bebedaa8b29a2f088c.
Strike Hupigon_debde42b	This strike sends a polymorphic malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Hupigon sample is debde42b74a9c09d210f40a2da174330.
Strike Hupigon_df65acf3	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is df65acf337ed114181b3c38deb258de5.
Strike Hupigon_df66e570	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is df66e570b2140d6bd39e75c7bbf26ed9.
Strike Hupigon_e921af12	This strike sends a malware sample known as Hupigon. The Hupigon malware are trojans that allow the remote user to execute commands on the system, such as to delete files and folders, download and execute files, and terminate processes. The MD5 hash of this Hupigon sample is e921af128394bc17536506a9ea7f1c13.
Strike HybridPetya_096dd6f0	This strike sends a malware sample known as HybridPetya. HybridPetya is a malware of the ransomware family that encrypts the Master File Table (MFT) of the NTFS file system, rendering the system unusable. It is delivered through a fake resume in a Dropbox link sent via email. Upon execution, it forces a system reboot and displays a fake check disk screen while it encrypts the MFT. Its key capabilities include encrypting the MFT, replacing the Master Boot Record (MBR) with a custom bootloader, and demanding a ransom to decrypt the system. The MD5 hash of this HybridPetya sample is 096dd6f0422ea562956e4eb64c48e311.

<b>Name</b>	<b>Description</b>
Strike HybridPetya_67051905	This strike sends a malware sample known as HybridPetya. HybridPetya is a malware of the ransomware family that encrypts the Master File Table (MFT) of the NTFS file system, rendering the system unusable. It is delivered through a fake resume in a Dropbox link sent via email. Upon execution, it forces a system reboot and displays a fake check disk screen while it encrypts the MFT. Its key capabilities include encrypting the MFT, replacing the Master Boot Record (MBR) with a custom bootloader, and demanding a ransom to decrypt the system. The MD5 hash of this HybridPetya sample is 670519058a309a63ff63bbf573f79916.
Strike HybridPetya_67e8ccae	This strike sends a malware sample known as HybridPetya. HybridPetya is a malware of the ransomware family that encrypts the Master File Table (MFT) of the NTFS file system, rendering the system unusable. It is delivered through a fake resume in a Dropbox link sent via email. Upon execution, it forces a system reboot and displays a fake check disk screen while it encrypts the MFT. Its key capabilities include encrypting the MFT, replacing the Master Boot Record (MBR) with a custom bootloader, and demanding a ransom to decrypt the system. The MD5 hash of this HybridPetya sample is 67e8ccaeecdce7983a40fc09d239945c4.
Strike HybridPetya_b1592068	This strike sends a malware sample known as HybridPetya. HybridPetya is a malware of the ransomware family that encrypts the Master File Table (MFT) of the NTFS file system, rendering the system unusable. It is delivered through a fake resume in a Dropbox link sent via email. Upon execution, it forces a system reboot and displays a fake check disk screen while it encrypts the MFT. Its key capabilities include encrypting the MFT, replacing the Master Boot Record (MBR) with a custom bootloader, and demanding a ransom to decrypt the system. The MD5 hash of this HybridPetya sample is b15920685a76992ad8179687b3c0a7c3.
Strike HybridPetya_baba1728	This strike sends a malware sample known as HybridPetya. HybridPetya is a malware of the ransomware family that encrypts the Master File Table (MFT) of the NTFS file system, rendering the system unusable. It is delivered through a fake resume in a Dropbox link sent via email. Upon execution, it forces a system reboot and displays a fake check disk screen while it encrypts the MFT. Its key capabilities include encrypting the MFT, replacing the Master Boot Record (MBR) with a custom bootloader, and demanding a ransom to decrypt the system. The MD5 hash of this HybridPetya sample is baba1728a03c8c05b13b57c909778c0a.
Strike HybridPetya_c6854118	This strike sends a malware sample known as HybridPetya. HybridPetya is a malware of the ransomware family that encrypts the Master File Table (MFT) of the NTFS file system, rendering the system unusable. It is delivered through a fake resume in a Dropbox link sent via email. Upon execution, it forces a system reboot and displays a fake check disk screen while it encrypts the MFT. Its key capabilities include encrypting the MFT, replacing the Master Boot Record (MBR) with a custom bootloader, and demanding a ransom to decrypt the system. The MD5 hash of this HybridPetya sample is c6854118f7e9ea0ec3cbd6163e3e2541.

<b>Name</b>	<b>Description</b>
Strike HybridPetya_e184fe6b	This strike sends a malware sample known as HybridPetya. HybridPetya is a malware of the ransomware family that encrypts the Master File Table (MFT) of the NTFS file system, rendering the system unusable. It is delivered through a fake resume in a Dropbox link sent via email. Upon execution, it forces a system reboot and displays a fake check disk screen while it encrypts the MFT. Its key capabilities include encrypting the MFT, replacing the Master Boot Record (MBR) with a custom bootloader, and demanding a ransom to decrypt the system. The MD5 hash of this HybridPetya sample is e184fe6b3244787a71e1d1d4a152a9b5.
Strike IZ1H9_20554f69	This strike sends a malware sample known as IZ1H9. IZ1H9, is a variant of Mirai, it targets Linux-based networked devices, particularly IoT devices, and transforms them into remotely controlled bots for conducting large-scale network attacks. The malware initiates a shell script downloader which proceeds to delete logs, download, and execute various bot clients for Linux architectures and obstruct network connections on multiple ports. It establishes C2 communication between compromised devices and the command sever, enabling the launching of DDoS attacks with specific parameters. The MD5 hash of this IZ1H9 sample is 20554f69078c318f92a4d89528318595.
Strike IZ1H9_34edf776	This strike sends a malware sample known as IZ1H9. IZ1H9, is a variant of Mirai, it targets Linux-based networked devices, particularly IoT devices, and transforms them into remotely controlled bots for conducting large-scale network attacks. The malware initiates a shell script downloader which proceeds to delete logs, download, and execute various bot clients for Linux architectures and obstruct network connections on multiple ports. It establishes C2 communication between compromised devices and the command sever, enabling the launching of DDoS attacks with specific parameters. The MD5 hash of this IZ1H9 sample is 34edf77604f651e56ad0ca346ecc2423.
Strike IZ1H9_92a88741	This strike sends a malware sample known as IZ1H9. IZ1H9, is a variant of Mirai, it targets Linux-based networked devices, particularly IoT devices, and transforms them into remotely controlled bots for conducting large-scale network attacks. The malware initiates a shell script downloader which proceeds to delete logs, download, and execute various bot clients for Linux architectures and obstruct network connections on multiple ports. It establishes C2 communication between compromised devices and the command sever, enabling the launching of DDoS attacks with specific parameters. The MD5 hash of this IZ1H9 sample is 92a887414c3dc1e56f72293918bd9ba4.
Strike IZ1H9_98edefbb	This strike sends a malware sample known as IZ1H9. IZ1H9, is a variant of Mirai, it targets Linux-based networked devices, particularly IoT devices, and transforms them into remotely controlled bots for conducting large-scale network attacks. The malware initiates a shell script downloader which proceeds to delete logs, download, and execute various bot clients for Linux architectures and obstruct network connections on multiple ports. It establishes C2 communication between compromised devices and the command sever, enabling the launching of DDoS attacks with specific parameters. The MD5 hash of this IZ1H9 sample is 98edefbbe07e13d7348c10c2773d3cba.

<b>Name</b>	<b>Description</b>
Strike IZ1H9_9f471c6d	This strike sends a malware sample known as IZ1H9. IZ1H9, is a variant of Mirai, it targets Linux-based networked devices, particularly IoT devices, and transforms them into remotely controlled bots for conducting large-scale network attacks. The malware initiates a shell script downloader which proceeds to delete logs, download, and execute various bot clients for Linux architectures and obstruct network connections on multiple ports. It establishes C2 communication between compromised devices and the command sever, enabling the launching of DDoS attacks with specific parameters. The MD5 hash of this IZ1H9 sample is 9f471c6d81cfccb1d13b9401a9ffd7b2.
Strike IZ1H9_9fbcdcd7e	This strike sends a malware sample known as IZ1H9. IZ1H9, is a variant of Mirai, it targets Linux-based networked devices, particularly IoT devices, and transforms them into remotely controlled bots for conducting large-scale network attacks. The malware initiates a shell script downloader which proceeds to delete logs, download, and execute various bot clients for Linux architectures and obstruct network connections on multiple ports. It establishes C2 communication between compromised devices and the command sever, enabling the launching of DDoS attacks with specific parameters. The MD5 hash of this IZ1H9 sample is 9fbcd7e36c9fd01085a96825d0bc186.
Strike IZ1H9_c0e82281	This strike sends a malware sample known as IZ1H9. IZ1H9, is a variant of Mirai, it targets Linux-based networked devices, particularly IoT devices, and transforms them into remotely controlled bots for conducting large-scale network attacks. The malware initiates a shell script downloader which proceeds to delete logs, download, and execute various bot clients for Linux architectures and obstruct network connections on multiple ports. It establishes C2 communication between compromised devices and the command sever, enabling the launching of DDoS attacks with specific parameters. The MD5 hash of this IZ1H9 sample is c0e82281a49e836a9ca75f44ca0749b5.
Strike IZ1H9_ca732733	This strike sends a malware sample known as IZ1H9. IZ1H9, is a variant of Mirai, it targets Linux-based networked devices, particularly IoT devices, and transforms them into remotely controlled bots for conducting large-scale network attacks. The malware initiates a shell script downloader which proceeds to delete logs, download, and execute various bot clients for Linux architectures and obstruct network connections on multiple ports. It establishes C2 communication between compromised devices and the command sever, enabling the launching of DDoS attacks with specific parameters. The MD5 hash of this IZ1H9 sample is ca732733cd816e60655c82bce09bc715.
Strike IZ1H9_d3dc81a5	This strike sends a malware sample known as IZ1H9. IZ1H9, is a variant of Mirai, it targets Linux-based networked devices, particularly IoT devices, and transforms them into remotely controlled bots for conducting large-scale network attacks. The malware initiates a shell script downloader which proceeds to delete logs, download, and execute various bot clients for Linux architectures and obstruct network connections on multiple ports. It establishes C2 communication between compromised devices and the command sever, enabling the launching of DDoS attacks with specific parameters. The MD5 hash of this IZ1H9 sample is d3dc81a5e1f00704c32fe8e5f79ab84f.

<b>Name</b>	<b>Description</b>
Strike IZ1H9_e06c85ea	<p>This strike sends a malware sample known as IZ1H9. IZ1H9, is a variant of Mirai, it targets Linux-based networked devices, particularly IoT devices, and transforms them into remotely controlled bots for conducting large-scale network attacks. The malware initiates a shell script downloader which proceeds to delete logs, download, and execute various bot clients for Linux architectures and obstruct network connections on multiple ports. It establishes C2 communication between compromised devices and the command sever, enabling the launching of DDoS attacks with specific parameters. The MD5 hash of this IZ1H9 sample is e06c85ea1da870053d4734a9ce52efa8.</p>
Strike IZ1H9_ec68eef6	<p>This strike sends a malware sample known as IZ1H9. IZ1H9, is a variant of Mirai, it targets Linux-based networked devices, particularly IoT devices, and transforms them into remotely controlled bots for conducting large-scale network attacks. The malware initiates a shell script downloader which proceeds to delete logs, download, and execute various bot clients for Linux architectures and obstruct network connections on multiple ports. It establishes C2 communication between compromised devices and the command sever, enabling the launching of DDoS attacks with specific parameters. The MD5 hash of this IZ1H9 sample is ec68eef6811d46791defa0cae0c04891.</p>
Strike InfectedSlurs_465e3c3f	<p>This strike sends a malware sample known as InfectedSlurs. InfectedSlurs is a new Mirai-based malware botnet that exploits two zero-day remote code execution vulnerabilities to infect routers and video recorder (NVR) devices. The malware hijacks these devices to form a distributed denial-of-service (DDoS) swarm, likely rented for profit. The malware is associated with the older JenX Mirai variant and poses a significant global threat, utilizing a unique approach of targeting a seldom-used TCP port. It particularly focuses on real-time streaming protocol (RTSP) enabled devices, exploiting a zero-day vulnerability in NVR devices and a second exploit in outlet-based wireless LAN routers designed for hotel and residential applications. The MD5 hash of this InfectedSlurs sample is 465e3c3fb87cd6402b162ae0777fceae.</p>
Strike InfectedSlurs_5cea697e	<p>This strike sends a malware sample known as InfectedSlurs. InfectedSlurs is a new Mirai-based malware botnet that exploits two zero-day remote code execution vulnerabilities to infect routers and video recorder (NVR) devices. The malware hijacks these devices to form a distributed denial-of-service (DDoS) swarm, likely rented for profit. The malware is associated with the older JenX Mirai variant and poses a significant global threat, utilizing a unique approach of targeting a seldom-used TCP port. It particularly focuses on real-time streaming protocol (RTSP) enabled devices, exploiting a zero-day vulnerability in NVR devices and a second exploit in outlet-based wireless LAN routers designed for hotel and residential applications. The MD5 hash of this InfectedSlurs sample is 5cea697e6eaf160d18987804be8d614a.</p>

<b>Name</b>	<b>Description</b>
Strike InfectedSlurs_71b4c3fe	<p>This strike sends a malware sample known as InfectedSlurs. InfectedSlurs is a new Mirai-based malware botnet that exploits two zero-day remote code execution vulnerabilities to infect routers and video recorder (NVR) devices. The malware hijacks these devices to form a distributed denial-of-service (DDoS) swarm, likely rented for profit. The malware is associated with the older JenX Mirai variant and poses a significant global threat, utilizing a unique approach of targeting a seldom-used TCP port. It particularly focuses on real-time streaming protocol (RTSP) enabled devices, exploiting a zero-day vulnerability in NVR devices and a second exploit in outlet-based wireless LAN routers designed for hotel and residential applications. The MD5 hash of this InfectedSlurs sample is 71b4c3fe502e6c6d5ef5e420d52d2729.</p>
Strike InfectedSlurs_7845a9a1	<p>This strike sends a malware sample known as InfectedSlurs. InfectedSlurs is a new Mirai-based malware botnet that exploits two zero-day remote code execution vulnerabilities to infect routers and video recorder (NVR) devices. The malware hijacks these devices to form a distributed denial-of-service (DDoS) swarm, likely rented for profit. The malware is associated with the older JenX Mirai variant and poses a significant global threat, utilizing a unique approach of targeting a seldom-used TCP port. It particularly focuses on real-time streaming protocol (RTSP) enabled devices, exploiting a zero-day vulnerability in NVR devices and a second exploit in outlet-based wireless LAN routers designed for hotel and residential applications. The MD5 hash of this InfectedSlurs sample is 7845a9a12131d48f2802f5bb310e22eb.</p>
Strike InfectedSlurs_84f587fe	<p>This strike sends a malware sample known as InfectedSlurs. InfectedSlurs is a new Mirai-based malware botnet that exploits two zero-day remote code execution vulnerabilities to infect routers and video recorder (NVR) devices. The malware hijacks these devices to form a distributed denial-of-service (DDoS) swarm, likely rented for profit. The malware is associated with the older JenX Mirai variant and poses a significant global threat, utilizing a unique approach of targeting a seldom-used TCP port. It particularly focuses on real-time streaming protocol (RTSP) enabled devices, exploiting a zero-day vulnerability in NVR devices and a second exploit in outlet-based wireless LAN routers designed for hotel and residential applications. The MD5 hash of this InfectedSlurs sample is 84f587fe72412ea24ad86fe182a66a98.</p>
Strike InfectedSlurs_89ddf5d8	<p>This strike sends a malware sample known as InfectedSlurs. InfectedSlurs is a new Mirai-based malware botnet that exploits two zero-day remote code execution vulnerabilities to infect routers and video recorder (NVR) devices. The malware hijacks these devices to form a distributed denial-of-service (DDoS) swarm, likely rented for profit. The malware is associated with the older JenX Mirai variant and poses a significant global threat, utilizing a unique approach of targeting a seldom-used TCP port. It particularly focuses on real-time streaming protocol (RTSP) enabled devices, exploiting a zero-day vulnerability in NVR devices and a second exploit in outlet-based wireless LAN routers designed for hotel and residential applications. The MD5 hash of this InfectedSlurs sample is 89ddf5d8c09a8f361dc7d22fd48bfeb3.</p>

<b>Name</b>	<b>Description</b>
Strike InfectedSlurs_8cafa4ae	<p>This strike sends a malware sample known as InfectedSlurs. InfectedSlurs is a new Mirai-based malware botnet that exploits two zero-day remote code execution vulnerabilities to infect routers and video recorder (NVR) devices. The malware hijacks these devices to form a distributed denial-of-service (DDoS) swarm, likely rented for profit. The malware is associated with the older JenX Mirai variant and poses a significant global threat, utilizing a unique approach of targeting a seldom-used TCP port. It particularly focuses on real-time streaming protocol (RTSP) enabled devices, exploiting a zero-day vulnerability in NVR devices and a second exploit in outlet-based wireless LAN routers designed for hotel and residential applications. The MD5 hash of this InfectedSlurs sample is 8cafa4aecaeedc2beb48dc083f1516dd.</p>
Strike InfectedSlurs_beca0315	<p>This strike sends a malware sample known as InfectedSlurs. InfectedSlurs is a new Mirai-based malware botnet that exploits two zero-day remote code execution vulnerabilities to infect routers and video recorder (NVR) devices. The malware hijacks these devices to form a distributed denial-of-service (DDoS) swarm, likely rented for profit. The malware is associated with the older JenX Mirai variant and poses a significant global threat, utilizing a unique approach of targeting a seldom-used TCP port. It particularly focuses on real-time streaming protocol (RTSP) enabled devices, exploiting a zero-day vulnerability in NVR devices and a second exploit in outlet-based wireless LAN routers designed for hotel and residential applications. The MD5 hash of this InfectedSlurs sample is beca0315899f617f4951f82922e3ed33.</p>
Strike InfectedSlurs_c00718ce	<p>This strike sends a malware sample known as InfectedSlurs. InfectedSlurs is a new Mirai-based malware botnet that exploits two zero-day remote code execution vulnerabilities to infect routers and video recorder (NVR) devices. The malware hijacks these devices to form a distributed denial-of-service (DDoS) swarm, likely rented for profit. The malware is associated with the older JenX Mirai variant and poses a significant global threat, utilizing a unique approach of targeting a seldom-used TCP port. It particularly focuses on real-time streaming protocol (RTSP) enabled devices, exploiting a zero-day vulnerability in NVR devices and a second exploit in outlet-based wireless LAN routers designed for hotel and residential applications. The MD5 hash of this InfectedSlurs sample is c00718ce5e0d0f2b5430d85480c4828f.</p>
Strike InfectedSlurs_cc888ace	<p>This strike sends a malware sample known as InfectedSlurs. InfectedSlurs is a new Mirai-based malware botnet that exploits two zero-day remote code execution vulnerabilities to infect routers and video recorder (NVR) devices. The malware hijacks these devices to form a distributed denial-of-service (DDoS) swarm, likely rented for profit. The malware is associated with the older JenX Mirai variant and poses a significant global threat, utilizing a unique approach of targeting a seldom-used TCP port. It particularly focuses on real-time streaming protocol (RTSP) enabled devices, exploiting a zero-day vulnerability in NVR devices and a second exploit in outlet-based wireless LAN routers designed for hotel and residential applications. The MD5 hash of this InfectedSlurs sample is cc888ace5a9ad90e95c7a08504a9de7f.</p>

<b>Name</b>	<b>Description</b>
Strike InfectedSlurs_d38aacc6	This strike sends a malware sample known as InfectedSlurs. InfectedSlurs is a new Mirai-based malware botnet that exploits two zero-day remote code execution vulnerabilities to infect routers and video recorder (NVR) devices. The malware hijacks these devices to form a distributed denial-of-service (DDoS) swarm, likely rented for profit. The malware is associated with the older JenX Mirai variant and poses a significant global threat, utilizing a unique approach of targeting a seldom-used TCP port. It particularly focuses on real-time streaming protocol (RTSP) enabled devices, exploiting a zero-day vulnerability in NVR devices and a second exploit in outlet-based wireless LAN routers designed for hotel and residential applications. The MD5 hash of this InfectedSlurs sample is d38aacc6becf788d30d5c709f497b518.
Strike InfectedSlurs_fadbed71	This strike sends a malware sample known as InfectedSlurs. InfectedSlurs is a new Mirai-based malware botnet that exploits two zero-day remote code execution vulnerabilities to infect routers and video recorder (NVR) devices. The malware hijacks these devices to form a distributed denial-of-service (DDoS) swarm, likely rented for profit. The malware is associated with the older JenX Mirai variant and poses a significant global threat, utilizing a unique approach of targeting a seldom-used TCP port. It particularly focuses on real-time streaming protocol (RTSP) enabled devices, exploiting a zero-day vulnerability in NVR devices and a second exploit in outlet-based wireless LAN routers designed for hotel and residential applications. The MD5 hash of this InfectedSlurs sample is fadbed7154b671c0d60493125d7c8d12.
Strike Injuke_04484ae9	This strike sends a malware sample known as Injuke. Injuke is a dropper that is known for retrieving other malware binaries. It can also communicate with remote servers to exfiltrate information from the victim machine. The MD5 hash of this Injuke sample is 04484ae93a15a6a6a8752bd960d15b1d.
Strike Injuke_07407dfb	This strike sends a malware sample known as Injuke. Injuke is a dropper that is known for retrieving other malware binaries. It can also communicate with remote servers to exfiltrate information from the victim machine. The MD5 hash of this Injuke sample is 07407dfb83110fef2c515d9a3058bf2c.
Strike Injuke_07d3c1d9	This strike sends a malware sample known as Injuke. Injuke is a dropper that is known for retrieving other malware binaries. It can also communicate with remote servers to exfiltrate information from the victim machine. The MD5 hash of this Injuke sample is 07d3c1d92bf0edcfcdc8ba71e3a130ff.
Strike Injuke_37bae635	This strike sends a malware sample known as Injuke. Injuke is a dropper that is known for retrieving other malware binaries. It can also communicate with remote servers to exfiltrate information from the victim machine. The MD5 hash of this Injuke sample is 37bae6357002a097632e925435bd0166.
Strike Injuke_39247ac6	This strike sends a malware sample known as Injuke. Injuke is a dropper that is known for retrieving other malware binaries. It can also communicate with remote servers to exfiltrate information from the victim machine. The MD5 hash of this Injuke sample is 39247ac6c0ada1e0a2fb038c24182b4.
Strike Injuke_4beed454	This strike sends a malware sample known as Injuke. Injuke is a dropper that is known for retrieving other malware binaries. It can also communicate with remote servers to exfiltrate information from the victim machine. The MD5 hash of this Injuke sample is 4beed454091bb6a752d12e7a658287ee.

<b>Name</b>	<b>Description</b>
Strike Injuke_5a771c67	This strike sends a malware sample known as Injuke. Injuke is a dropper that is known for retrieving other malware binaries. It can also communicate with remote servers to exfiltrate information from the victim machine. The MD5 hash of this Injuke sample is 5a771c67b82cf9cd1778d87ad88b6cb2.
Strike Injuke_a6b60939	This strike sends a malware sample known as Injuke. Injuke is a dropper that is known for retrieving other malware binaries. It can also communicate with remote servers to exfiltrate information from the victim machine. The MD5 hash of this Injuke sample is a6b60939fd4519c50856072670b82648.
Strike Injuke_be7e7bc0	This strike sends a malware sample known as Injuke. Injuke is a dropper that is known for retrieving other malware binaries. It can also communicate with remote servers to exfiltrate information from the victim machine. The MD5 hash of this Injuke sample is be7e7bc0b0025b091457629493d1a982.
Strike Injuke_c6eb0bd1	This strike sends a malware sample known as Injuke. Injuke is a dropper that is known for retrieving other malware binaries. It can also communicate with remote servers to exfiltrate information from the victim machine. The MD5 hash of this Injuke sample is c6eb0bd166bc638bbdbcc7bc053f37da.
Strike Injuke_d997417e	This strike sends a malware sample known as Injuke. Injuke is a dropper that is known for retrieving other malware binaries. It can also communicate with remote servers to exfiltrate information from the victim machine. The MD5 hash of this Injuke sample is d997417e7acf295ab65d445ee3a8789c.
Strike Injuke_f1fd1462	This strike sends a malware sample known as Injuke. Injuke is a dropper that is known for retrieving other malware binaries. It can also communicate with remote servers to exfiltrate information from the victim machine. The MD5 hash of this Injuke sample is f1fd1462c56f822ccba61454ab7d44ed.
Strike JanelaRAT_172ca00d	This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is 172ca00d32a201f5e917bc4d73f720a1.

<b>Name</b>	<b>Description</b>
Strike JanelaRAT_1b72c12d	<p>This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is 1b72c12db8a37103a37cab5b3b14398c.</p>
Strike JanelaRAT_3870e4a4	<p>This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is 3870e4a4d86a34424ea47bdaa722cd89.</p>
Strike JanelaRAT_397e407e	<p>This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is 397e407e63128e71089971e3b35dd253.</p>
Strike JanelaRAT_44d9f29a	<p>This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is 44d9f29a81a2f2df83b6000165e8a06f.</p>

<b>Name</b>	<b>Description</b>
Strike JanelaRAT_48c189e5	<p>This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is 48c189e5dfe28b9d2b32fd813a991adb.</p>
Strike JanelaRAT_505fab6d	<p>This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is 505fab6d83ef86a4b12b5808047fa7f1.</p>
Strike JanelaRAT_691cc21d	<p>This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is 691cc21dae6e320564f74d6372e94286.</p>
Strike JanelaRAT_81618be6	<p>This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is 81618be603bca301ac156ed169444569.</p>

<b>Name</b>	<b>Description</b>
Strike JanelaRAT_84919bf0	<p>This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is 84919bf0583c0e6c04e606f34a1d56f3.</p>
Strike JanelaRAT_900445a5	<p>This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is 900445a57f462d0df130c3612e6caed7.</p>
Strike JanelaRAT_ba2bd2d3	<p>This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is ba2bd2d31cf591480b69e106b0e77b5c.</p>
Strike JanelaRAT_c86fdacd	<p>This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is c86fdacd8af28cb08ef406bc6d4fc5a7.</p>

<b>Name</b>	<b>Description</b>
Strike JanelaRAT_d1684fa8	This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is d1684fa84602a2d560b47dfe0f0779b4.
Strike JanelaRAT_f71471d7	This strike sends a malware sample known as JanelaRAT. JanelaRAT malware has been discovered targeting financial and cryptocurrency data from financial institutions. The malware is a multi staged malware with the original infection being unknown. It begins as a compressed archive that contains a VBS script. Once executed the VBS script drops a batch script and retrieves an additional compressed archive from the attacker. The batch script sets up persistence on the machine. The RAT includes the capability to record mouse and keyboard inputs and record screenshots. One of the key tasks of the malware is to capture the content of the windows title bars to check for relevant titles that may indicate a financial target. JanelaRAT uses a legitimate DLL to side load a malicious dll, and communicates with an attacker controlled C2 server. The MD5 hash of this JanelaRAT sample is f71471d7e94ef739a8ee44125023b750.
Strike Johnnie_006d8728	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 006d8728a4620369481696802a18b6ae.
Strike Johnnie_00826892	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 0082689270c8db3432602ace4edb0ad2.
Strike Johnnie_0318ec7b	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 0318ec7b3f61394e00293704921dd4c6.
Strike Johnnie_15459468	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 15459468e06d5d7a87da077876f8f92c.
Strike Johnnie_1bfd9858	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 1bfd985899f6a9d83478eb869df273d1.
Strike Johnnie_3489533a	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 3489533aef88a0ebbf18393459d212b0.

<b>Name</b>	<b>Description</b>
Strike Johnnie_38887b35	This strike sends a polymorphic malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Johnnie sample is 38887b351d676a1a552cb3c9af280e90.
Strike Johnnie_38c0b11f	This strike sends a polymorphic malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The binary has the debug flag removed in the PE file format. The MD5 hash of this Johnnie sample is 38c0b11fddbfbcc2806cfacb08ecd6ca1.
Strike Johnnie_414e319d	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 414e319d8a4769b01b783bb2c7297449.
Strike Johnnie_44a08a4a	This strike sends a polymorphic malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Johnnie sample is 44a08a4a0e364cf65eae97000baffd06.
Strike Johnnie_44a6f92e	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 44a6f92e70e8e011d6e39dbfc387157b.
Strike Johnnie_473f83f1	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 473f83f197ba26d4599757b81ce0dd52.
Strike Johnnie_573c737a	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 573c737af7ee30678c11ec775ce9bca9.
Strike Johnnie_5a66dd86	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 5a66dd86de39a4eaf55ded4320a8ff43.
Strike Johnnie_61477e80	This strike sends a polymorphic malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Johnnie sample is 61477e80eec0c78d674edb9798ffef5.
Strike Johnnie_707cc8ef	This strike sends a polymorphic malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The binary has the debug flag removed in the PE file format. The MD5 hash of this Johnnie sample is 707cc8ef9a179285e235974314c3449e.
Strike Johnnie_7236d785	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 7236d785527143086ea1e77b3e975342.

<b>Name</b>	<b>Description</b>
Strike Johnnie_7583af11	This strike sends a polymorphic malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The binary has random bytes appended at the end of the file. The MD5 hash of this Johnnie sample is 7583af11e00d12f390a15c3fe33a4b4f.
Strike Johnnie_7a526e82	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 7a526e82d6249af223c93a4bad5629bf.
Strike Johnnie_7e1abfa8	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 7e1abfa80d07ed765c6325f18e024246.
Strike Johnnie_81c7f75d	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 81c7f75dea4d7583fe012af46c343717.
Strike Johnnie_823ae99b	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 823ae99b9a63bea70795d4aeb40373d2.
Strike Johnnie_8e1b7f46	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 8e1b7f46cf344b314299c80919c1ef33.
Strike Johnnie_93d523a8	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 93d523a8b43d457b5406fcb6320d0f58.
Strike Johnnie_9bd611de	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is 9bd611decef5a788290814c6f4236cb2.
Strike Johnnie_a14f71fe	This strike sends a polymorphic malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The binary has the checksum removed in the PE file format. The MD5 hash of this Johnnie sample is a14f71fe7ea29bb40ad88b302881dab6.
Strike Johnnie_a2701860	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is a27018604fc28b1b3becb277e770ba09.
Strike Johnnie_a2e7a4af	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is a2e7a4afaad0d86de5deb1d4a273d6ab.

<b>Name</b>	<b>Description</b>
Strike Johnnie_a31b0f6e	This strike sends a polymorphic malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Johnnie sample is a31b0f6e146fc15ebbc5b147b3f097c5.
Strike Johnnie_a338cd03	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is a338cd032054e9146ee5b8ebd99f9e58.
Strike Johnnie_ab5fa6b3	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is ab5fa6b31ab7c53af696f3c235675498.
Strike Johnnie_ac4c707d	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is ac4c707dc7839f5f587225bfe3ec2fde.
Strike Johnnie_add45c04	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is add45c044a3c692d3c7a5bc5fe383751.
Strike Johnnie_b20dcf58	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is b20dcf58c0cfb67f1fe389302e033d4f.
Strike Johnnie_b39fc516	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is b39fc51671033a3abefdb125a58ffd14.
Strike Johnnie_b3de3cd3	This strike sends a polymorphic malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Johnnie sample is b3de3cd3f7f35383af885a9daceda7e1.
Strike Johnnie_b522d0cf	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is b522d0cf76121d9e4fcc1ba12718ce3c.
Strike Johnnie_b5435aca	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is b5435aca01e6f182ec43d92e86c73f0.
Strike Johnnie_bb97ffe2	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is bb97ffe2b81520714594a1a4a0fbf161.

<b>Name</b>	<b>Description</b>
Strike Johnnie_be0e6047	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is be0e6047078cdce823e27cf0ff8a5ee.
Strike Johnnie_cb652b95	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is cb652b95e5fe643cda5838279a73c3e6.
Strike Johnnie_cfe3f1b2	This strike sends a polymorphic malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Johnnie sample is cfe3f1b25bf77334bef22e6db871358b.
Strike Johnnie_d2fd1878	This strike sends a polymorphic malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The binary has random bytes appended at the end of the file. The MD5 hash of this Johnnie sample is d2fd187823f6e78e1967b1cf04dac07f.
Strike Johnnie_dc7e8f77	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is dc7e8f77cbbd7450502f7ffe563cb7bb.
Strike Johnnie_dcf7af3e	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is dcf7af3ecdaff092c3649383e9baecc4.
Strike Johnnie_debdb48b	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is debdb48baba37bc651ecd823605cd46c.
Strike Johnnie_e0079301	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is e0079301b101c37ff3e5b8f424e92faa.
Strike Johnnie_e09ba79a	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is e09ba79a177bf796e44b10f67cc45d8f.
Strike Johnnie_e429ec31	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is e429ec317e88a45ffe3338aeee9fe11c.
Strike Johnnie_e6faa2e3	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is e6faa2e3d72d4a8cbbff122b335e72a0.

<b>Name</b>	<b>Description</b>
Strike Johnnie_ee9b176e	This strike sends a polymorphic malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Johnnie sample is ee9b176eef23f5a4e9a759f80de3f3a0.
Strike Johnnie_f4805a5a	This strike sends a malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The MD5 hash of this Johnnie sample is f4805a5a3e898264b8ed4b43de37b60b.
Strike Johnnie_f492468b	This strike sends a polymorphic malware sample known as Johnnie. Johnnie, also known as Mikey, is a malware family that focuses on persistence and is known for its plugin architecture. The binary has the checksum removed in the PE file format. The MD5 hash of this Johnnie sample is f492468be9b84083fc48b102b9ce1fa.
Strike Joker_0b9911cc	This strike sends a malware sample known as Joker. Joker is a billing fraud family of malware. It looks like a legitimate app, and often times bypasses Google Play's security protections. Once executed it steals SMS messages, contact lists and device information; as well as signs the victim up for premium service subscriptions to siphon money. Recent variants hide malicious code inside the Android Manifest of a legitimate application. The MD5 hash of this Joker sample is 0b9911ccb089c7ab5ad8a0cbbe25c700.
Strike Joker_2a7d3d07	This strike sends a malware sample known as Joker. Joker is a billing fraud family of malware. It looks like a legitimate app, and often times bypasses Google Play's security protections. Once executed it steals SMS messages, contact lists and device information; as well as signs the victim up for premium service subscriptions to siphon money. Recent variants hide malicious code inside the Android Manifest of a legitimate application. The MD5 hash of this Joker sample is 2a7d3d0734f31eb11397cef2b49225c7.
Strike Joker_3c5abec5	This strike sends a malware sample known as Joker. Joker is a billing fraud family of malware. It looks like a legitimate app, and often times bypasses Google Play's security protections. Once executed it steals SMS messages, contact lists and device information; as well as signs the victim up for premium service subscriptions to siphon money. Recent variants hide malicious code inside the Android Manifest of a legitimate application. The MD5 hash of this Joker sample is 3c5abec5b685809a670dee9b729a9096.
Strike Joker_6d0e6a88	This strike sends a malware sample known as Joker. Joker is a billing fraud family of malware. It looks like a legitimate app, and often times bypasses Google Play's security protections. Once executed it steals SMS messages, contact lists and device information; as well as signs the victim up for premium service subscriptions to siphon money. Recent variants hide malicious code inside the Android Manifest of a legitimate application. The MD5 hash of this Joker sample is 6d0e6a88f5ec092de6045ac4a5e6219d.
Strike Joker_87d70b11	This strike sends a malware sample known as Joker. Joker is a billing fraud family of malware. It looks like a legitimate app, and often times bypasses Google Play's security protections. Once executed it steals SMS messages, contact lists and device information; as well as signs the victim up for premium service subscriptions to siphon money. Recent variants hide malicious code inside the Android Manifest of a legitimate application. The MD5 hash of this Joker sample is 87d70b118d68b5b8630d09ca3c2083ae.

<b>Name</b>	<b>Description</b>
Strike Joker_966daec1	This strike sends a malware sample known as Joker. Joker is a billing fraud family of malware. It looks like a legitimate app, and often times bypasses Google Play's security protections. Once executed it steals SMS messages, contact lists and device information; as well as signs the victim up for premium service subscriptions to siphon money. Recent variants hide malicious code inside the Android Manifest of a legitimate application. The MD5 hash of this Joker sample is 966daec16869c8bbdfb1243dfc115712.
Strike Joker_b0dce678	This strike sends a malware sample known as Joker. Joker is a billing fraud family of malware. It looks like a legitimate app, and often times bypasses Google Play's security protections. Once executed it steals SMS messages, contact lists and device information; as well as signs the victim up for premium service subscriptions to siphon money. Recent variants hide malicious code inside the Android Manifest of a legitimate application. The MD5 hash of this Joker sample is b0dce6785bb79f271611b69a7ea81f71.
Strike Joker_baa1ecdd	This strike sends a malware sample known as Joker. Joker is a billing fraud family of malware. It looks like a legitimate app, and often times bypasses Google Play's security protections. Once executed it steals SMS messages, contact lists and device information; as well as signs the victim up for premium service subscriptions to siphon money. Recent variants hide malicious code inside the Android Manifest of a legitimate application. The MD5 hash of this Joker sample is baa1ecdd95d6a13551f783b715cb19ae.
Strike Joker_c8e8080c	This strike sends a malware sample known as Joker. Joker is a billing fraud family of malware. It looks like a legitimate app, and often times bypasses Google Play's security protections. Once executed it steals SMS messages, contact lists and device information; as well as signs the victim up for premium service subscriptions to siphon money. Recent variants hide malicious code inside the Android Manifest of a legitimate application. The MD5 hash of this Joker sample is c8e8080c1365da6dc340edc17d86f674.
Strike Joker_d1a2ee8a	This strike sends a malware sample known as Joker. Joker is a billing fraud family of malware. It looks like a legitimate app, and often times bypasses Google Play's security protections. Once executed it steals SMS messages, contact lists and device information; as well as signs the victim up for premium service subscriptions to siphon money. Recent variants hide malicious code inside the Android Manifest of a legitimate application. The MD5 hash of this Joker sample is d1a2ee8a66fa0d90477e29cc35a84ba9.
Strike Kaden_12fbcbef	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is 12fbcbef445e1fadfe40081117626a17.
Strike Kaden_1390c057	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is 1390c057426987f42095d4a3f2aab309.

<b>Name</b>	<b>Description</b>
Strike Kaden_2e4771f3	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is 2e4771f338a9ee73662c1bc8e5170a59.
Strike Kaden_4733fe39	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is 4733fe39135798035d67d53f8ee1344e.
Strike Kaden_50fecc43	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is 50fecc437e5a9048f82066d6a57ff2f9.
Strike Kaden_5d50f3b8	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is 5d50f3b866987905e677b9e903ac811f.
Strike Kaden_663c2ff8	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is 663c2ff84dc328e963457589beb348b5.
Strike Kaden_6846627f	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is 6846627ff63bdc09c11abfc15d8bf3ad.
Strike Kaden_6fa65771	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is 6fa65771f203534d68b50b0f77e07c42.
Strike Kaden_70d3d1fd	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is 70d3d1fd74a38a7cfb7600bfb2f44ce4.
Strike Kaden_7dfb0813	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is 7dfb08131dc695f43545cca5f0d77f5c.

<b>Name</b>	<b>Description</b>
Strike Kaden_8b299823	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is 8b299823fa88250ea7b8ae8a1b116220.
Strike Kaden_99b5721e	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is 99b5721e20397b498abfad313f03b8ff.
Strike Kaden_b506b4d1	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is b506b4d132a28748e4341aff010c2325.
Strike Kaden_f8113c0e	This strike sends a malware sample known as Kaden. Kaden is a botnet that exhibits various functions and elements from other botnets like Gafgyt. Some of the botnet commands include HTTP and UDP flood attacks, removing logs and recent variants include wiping capabilities. The MD5 hash of this Kaden sample is f8113c0e710553d924da955bb6596cc3.
Strike KandyKorn_015c5d12	This strike sends a malware sample known as KandyKorn. KandyKorn is a sophisticated multi-stage malware campaign orchestrated by DPRK threat actors, targeting blockchain engineers of a crypto exchange platform. This operation employs Python scripts to initially compromise the Discord app, leading to the delivery of the C++ based backdoor RAT. The campaign utilizes social engineering through Discord, enticing victims with a malicious Python application disguised as a cryptocurrency tool. The malware's modular approach includes SwiftLoader droppers, and its capabilities involve script execution, Mach-O binary deployment, and communication with remote C2 servers for data exfiltration. The MD5 hash of this KandyKorn sample is 015c5d12273dde42fd0a17985ee9a1cd.
Strike KandyKorn_056b1d9c	This strike sends a malware sample known as KandyKorn. KandyKorn is a sophisticated multi-stage malware campaign orchestrated by DPRK threat actors, targeting blockchain engineers of a crypto exchange platform. This operation employs Python scripts to initially compromise the Discord app, leading to the delivery of the C++ based backdoor RAT. The campaign utilizes social engineering through Discord, enticing victims with a malicious Python application disguised as a cryptocurrency tool. The malware's modular approach includes SwiftLoader droppers, and its capabilities involve script execution, Mach-O binary deployment, and communication with remote C2 servers for data exfiltration. The MD5 hash of this KandyKorn sample is 056b1d9ce628efe6128e17cddab3811e.

<b>Name</b>	<b>Description</b>
Strike KandyKorn_2df15cbc	<p>This strike sends a malware sample known as KandyKorn. KandyKorn is a sophisticated multi-stage malware campaign orchestrated by DPRK threat actors, targeting blockchain engineers of a crypto exchange platform. This operation employs Python scripts to initially compromise the Discord app, leading to the delivery of the C++ based backdoor RAT. The campaign utilizes social engineering through Discord, enticing victims with a malicious Python application disguised as a cryptocurrency tool. The malware's modular approach includes SwiftLoader droppers, and its capabilities involve script execution, Mach-O binary deployment, and communication with remote C2 servers for data exfiltration. The MD5 hash of this KandyKorn sample is 2df15cbc4367b5806e8a3c6abf88abdf.</p>
Strike KandyKorn_447fa714	<p>This strike sends a malware sample known as KandyKorn. KandyKorn is a sophisticated multi-stage malware campaign orchestrated by DPRK threat actors, targeting blockchain engineers of a crypto exchange platform. This operation employs Python scripts to initially compromise the Discord app, leading to the delivery of the C++ based backdoor RAT. The campaign utilizes social engineering through Discord, enticing victims with a malicious Python application disguised as a cryptocurrency tool. The malware's modular approach includes SwiftLoader droppers, and its capabilities involve script execution, Mach-O binary deployment, and communication with remote C2 servers for data exfiltration. The MD5 hash of this KandyKorn sample is 447fa7141877e0f01fa191b70791dfbf.</p>
Strike KandyKorn_541341fc	<p>This strike sends a malware sample known as KandyKorn. KandyKorn is a sophisticated multi-stage malware campaign orchestrated by DPRK threat actors, targeting blockchain engineers of a crypto exchange platform. This operation employs Python scripts to initially compromise the Discord app, leading to the delivery of the C++ based backdoor RAT. The campaign utilizes social engineering through Discord, enticing victims with a malicious Python application disguised as a cryptocurrency tool. The malware's modular approach includes SwiftLoader droppers, and its capabilities involve script execution, Mach-O binary deployment, and communication with remote C2 servers for data exfiltration. The MD5 hash of this KandyKorn sample is 541341fc477523fed26e8b7edec1c6bb.</p>
Strike KandyKorn_5d0df3f5	<p>This strike sends a malware sample known as KandyKorn. KandyKorn is a sophisticated multi-stage malware campaign orchestrated by DPRK threat actors, targeting blockchain engineers of a crypto exchange platform. This operation employs Python scripts to initially compromise the Discord app, leading to the delivery of the C++ based backdoor RAT. The campaign utilizes social engineering through Discord, enticing victims with a malicious Python application disguised as a cryptocurrency tool. The malware's modular approach includes SwiftLoader droppers, and its capabilities involve script execution, Mach-O binary deployment, and communication with remote C2 servers for data exfiltration. The MD5 hash of this KandyKorn sample is 5d0df3f506138b4ba7c7bb1f22b3abd5.</p>

<b>Name</b>	<b>Description</b>
Strike KandyKorn_749da6c3	<p>This strike sends a malware sample known as KandyKorn. KandyKorn is a sophisticated multi-stage malware campaign orchestrated by DPRK threat actors, targeting blockchain engineers of a crypto exchange platform. This operation employs Python scripts to initially compromise the Discord app, leading to the delivery of the C++ based backdoor RAT. The campaign utilizes social engineering through Discord, enticing victims with a malicious Python application disguised as a cryptocurrency tool. The malware's modular approach includes SwiftLoader droppers, and its capabilities involve script execution, Mach-O binary deployment, and communication with remote C2 servers for data exfiltration. The MD5 hash of this KandyKorn sample is 749da6c3a50f60f3636443275118b20f.</p>
Strike KandyKorn_973225dc	<p>This strike sends a malware sample known as KandyKorn. KandyKorn is a sophisticated multi-stage malware campaign orchestrated by DPRK threat actors, targeting blockchain engineers of a crypto exchange platform. This operation employs Python scripts to initially compromise the Discord app, leading to the delivery of the C++ based backdoor RAT. The campaign utilizes social engineering through Discord, enticing victims with a malicious Python application disguised as a cryptocurrency tool. The malware's modular approach includes SwiftLoader droppers, and its capabilities involve script execution, Mach-O binary deployment, and communication with remote C2 servers for data exfiltration. The MD5 hash of this KandyKorn sample is 973225dc83f568ef6208d49fe2648fc0.</p>
Strike KandyKorn_a4963b1b	<p>This strike sends a malware sample known as KandyKorn. KandyKorn is a sophisticated multi-stage malware campaign orchestrated by DPRK threat actors, targeting blockchain engineers of a crypto exchange platform. This operation employs Python scripts to initially compromise the Discord app, leading to the delivery of the C++ based backdoor RAT. The campaign utilizes social engineering through Discord, enticing victims with a malicious Python application disguised as a cryptocurrency tool. The malware's modular approach includes SwiftLoader droppers, and its capabilities involve script execution, Mach-O binary deployment, and communication with remote C2 servers for data exfiltration. The MD5 hash of this KandyKorn sample is a4963b1b9468027d78273e86a1793c1b.</p>
Strike KandyKorn_b58dce1b	<p>This strike sends a malware sample known as KandyKorn. KandyKorn is a sophisticated multi-stage malware campaign orchestrated by DPRK threat actors, targeting blockchain engineers of a crypto exchange platform. This operation employs Python scripts to initially compromise the Discord app, leading to the delivery of the C++ based backdoor RAT. The campaign utilizes social engineering through Discord, enticing victims with a malicious Python application disguised as a cryptocurrency tool. The malware's modular approach includes SwiftLoader droppers, and its capabilities involve script execution, Mach-O binary deployment, and communication with remote C2 servers for data exfiltration. The MD5 hash of this KandyKorn sample is b58dce1b81357a78b49546468f3adbe1.</p>

<b>Name</b>	<b>Description</b>
Strike KandyKorn_e4539403	<p>This strike sends a malware sample known as KandyKorn. KandyKorn is a sophisticated multi-stage malware campaign orchestrated by DPRK threat actors, targeting blockchain engineers of a crypto exchange platform. This operation employs Python scripts to initially compromise the Discord app, leading to the delivery of the C++ based backdoor RAT. The campaign utilizes social engineering through Discord, enticing victims with a malicious Python application disguised as a cryptocurrency tool. The malware's modular approach includes SwiftLoader droppers, and its capabilities involve script execution, Mach-O binary deployment, and communication with remote C2 servers for data exfiltration. The MD5 hash of this KandyKorn sample is e45394036e56637192bcc44d02bb00d9.</p>
Strike KandyKorn_f8fdfb1d	<p>This strike sends a malware sample known as KandyKorn. KandyKorn is a sophisticated multi-stage malware campaign orchestrated by DPRK threat actors, targeting blockchain engineers of a crypto exchange platform. This operation employs Python scripts to initially compromise the Discord app, leading to the delivery of the C++ based backdoor RAT. The campaign utilizes social engineering through Discord, enticing victims with a malicious Python application disguised as a cryptocurrency tool. The malware's modular approach includes SwiftLoader droppers, and its capabilities involve script execution, Mach-O binary deployment, and communication with remote C2 servers for data exfiltration. The MD5 hash of this KandyKorn sample is f8fdfb1d21eaebaee117b041d42447a.</p>
Strike Kapeka_169cbeb9	<p>This strike sends a polymorphic malware sample known as Kapeka. Kapeka is malware that acts as backdoor that has been linked to a threat actor group known as Sandworm. The malware has a dropper that drops and then executes the backdoor. Once executed it will send system information back to the attackers. The binary has been packed using upx packer, with the default options. The MD5 hash of this Kapeka sample is 169cbeb980924f190b290c14fd2b068d.</p>
Strike Kapeka_2befbf05a	<p>This strike sends a malware sample known as Kapeka. Kapeka is malware that acts as backdoor that has been linked to a threat actor group known as Sandworm. The malware has a dropper that drops and then executes the backdoor. Once executed it will send system information back to the attackers. The MD5 hash of this Kapeka sample is 2befbf05a9607f038f5407248fb075cd6.</p>
Strike Kapeka_3a4c7bbf	<p>This strike sends a polymorphic malware sample known as Kapeka. Kapeka is malware that acts as backdoor that has been linked to a threat actor group known as Sandworm. The malware has a dropper that drops and then executes the backdoor. Once executed it will send system information back to the attackers. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Kapeka sample is 3a4c7bbf1e9a081bd88471c84bb51d47.</p>
Strike Kapeka_50acd887	<p>This strike sends a polymorphic malware sample known as Kapeka. Kapeka is malware that acts as backdoor that has been linked to a threat actor group known as Sandworm. The malware has a dropper that drops and then executes the backdoor. Once executed it will send system information back to the attackers. The binary has the debug flag removed in the PE file format. The MD5 hash of this Kapeka sample is 50acd88764970f708a69a3117a4ffaf6.</p>

<b>Name</b>	<b>Description</b>
Strike Kapeka_50b55829	This strike sends a malware sample known as Kapeka. Kapeka is malware that acts as backdoor that has been linked to a threat actor group known as Sandworm. The malware has a dropper that drops and then executes the backdoor. Once executed it will send system information back to the attackers. The MD5 hash of this Kapeka sample is 50b5582904fe34451f5cb2362e11cb24.
Strike Kapeka_5294AAF2	This strike sends a malware sample known as Kapeka. Kapeka is malware that acts as backdoor that has been linked to a threat actor group known as Sandworm. The malware has a dropper that drops and then executes the backdoor. Once executed it will send system information back to the attackers. The MD5 hash of this Kapeka sample is 5294AAF2ff80547172ebb9e0bcb52e0f.
Strike Kapeka_6b65a179	This strike sends a polymorphic malware sample known as Kapeka. Kapeka is malware that acts as backdoor that has been linked to a threat actor group known as Sandworm. The malware has a dropper that drops and then executes the backdoor. Once executed it will send system information back to the attackers. The binary has random bytes appended at the end of the file. The MD5 hash of this Kapeka sample is 6b65a1791a5ee26116b996edd4026ac3.
Strike Kapeka_7bf64fcc	This strike sends a polymorphic malware sample known as Kapeka. Kapeka is malware that acts as backdoor that has been linked to a threat actor group known as Sandworm. The malware has a dropper that drops and then executes the backdoor. Once executed it will send system information back to the attackers. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Kapeka sample is 7bf64fcc7865a8b3954fce6c436a9901.
Strike Kapeka_953da973	This strike sends a polymorphic malware sample known as Kapeka. Kapeka is malware that acts as backdoor that has been linked to a threat actor group known as Sandworm. The malware has a dropper that drops and then executes the backdoor. Once executed it will send system information back to the attackers. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Kapeka sample is 953da9738083f8c3cbe7817633621da5.
Strike Kapeka_d8f9c24a	This strike sends a polymorphic malware sample known as Kapeka. Kapeka is malware that acts as backdoor that has been linked to a threat actor group known as Sandworm. The malware has a dropper that drops and then executes the backdoor. Once executed it will send system information back to the attackers. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Kapeka sample is d8f9c24ab8cd2d74aa4ce5aa52e70538.
Strike Katz_02115d00	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 02115d0005c8ade176156c78565828dc.
Strike Katz_0710c5fd	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 0710c5fd7d53dece6926b297e343d3f2.

<b>Name</b>	<b>Description</b>
Strike Katz_07a7f829	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 07a7f829677af65f778369a3fc4e1f86.
Strike Katz_081f29e7	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 081f29e70ee9fc5c98670eb874871547.
Strike Katz_151ab8a4	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 151ab8a4cc1d5b1995e15c3ca19baff9.
Strike Katz_1ad13ba8	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 1ad13ba816a63bcf1d01c8485f500029.
Strike Katz_1f86370a	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 1f86370a6a8f6c2757a9f369efdfd52d.
Strike Katz_2644ca19	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 2644ca19399ceb0826ab0bf63af00577.
Strike Katz_2e93e90d	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 2e93e90db74c9c9a606a5cd8e80fce5e.
Strike Katz_3272a23d	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 3272a23dc07e137402aafcdeb25397d4.
Strike Katz_3786bf65	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 3786bf65df20165b526af646ab1e46c7.
Strike Katz_38331f13	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 38331f134a3f5ee9a945c2d1d4f0768a.

<b>Name</b>	<b>Description</b>
Strike Katz_3f3ada87	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 3f3ada874a48e48d72ac26d12f8c7e60.
Strike Katz_5249739c	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 5249739c4049a32207828449671f0faa.
Strike Katz_542b3f94	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 542b3f9462113c46ec44b0fe6b0681d1.
Strike Katz_63368017	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 6336801701845edb81946b42876a20ac.
Strike Katz_68379cae	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 68379cae8fcb5fc5c29b831727b53c63.
Strike Katz_6bcae382	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 6bcae3827c4a9015319553188ae52edf.
Strike Katz_73462631	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 73462631872be6fb456063f9a7718d6c.
Strike Katz_74a7b0e5	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 74a7b0e5438b16326b9230aea2a5b359.
Strike Katz_7b1b9f02	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 7b1b9f0292979cf0df3ef21f4bae0882.
Strike Katz_829f1399	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 829f139966ebe28189dbe3eca8c7296.

<b>Name</b>	<b>Description</b>
Strike Katz_848a89e1	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 848a89e10ff33aae1b4ecf360a1cb1ce.
Strike Katz_8e7ded00	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 8e7ded0089b6adfd951b5d8175078f7.
Strike Katz_90c5821b	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 90c5821bf41c4ab7f33bb748551def22.
Strike Katz_94b5e34b	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 94b5e34bef3d836632ef422205c5c1f3.
Strike Katz_98eb2f36	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 98eb2f36b29ae6ae48640b742c8efd63.
Strike Katz_9dca6162	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is 9dca61626ab6343fb5e39ce310b367e8.
Strike Katz_a3727ff6	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is a3727ff64c82935d7697e3fefc6af383.
Strike Katz_a672f39e	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is a672f39ead8bd2f98386bb9b62c708a2.
Strike Katz_b52ace1f	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is b52ace1f26aab3fbf89ee9fb8d23a52e.
Strike Katz_baf29279	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is baf292797b6d10fadbd32f4ebcd575587.

<b>Name</b>	<b>Description</b>
Strike Katz_bb2b3420	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is bb2b3420577efcc0c0a09f7488456b91.
Strike Katz_cd1dd021	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is cd1dd021e439fd621fc3410fb2dfb78.
Strike Katz_d384268b	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is d384268b339c7e5440ee1a7607be3495.
Strike Katz_da7ec01e	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is da7ec01e2e6a198d1968055642ec5012.
Strike Katz_e1c6f609	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is e1c6f609d713913f8c4ea4b7ff4837f3.
Strike Katz_e5d9896e	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is e5d9896e98ac498a76cf4fa4c13f4d04.
Strike Katz_e9b413e1	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is e9b413e1abd01b6b98062d39c5552a57.
Strike Katz_eff3042e	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is eff3042e5f5483212c90dbc70033ed74.
Strike Katz_f0220f5d	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is f0220f5d1f935f09d58e869247cfdb5d.
Strike Katz_f175f4c2	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is f175f4c2d99cc4f35f9aecdfffc3489ed.

<b>Name</b>	<b>Description</b>
Strike Katz_f69bf1ed	This strike sends a malware sample known as Katz. Katz Stealer malware is a credential stealer that offers its services for many popular communication platforms like Discord, Slack, Signal, Teams etc. The MD5 hash of this Katz sample is f69bf1ed39691a1c5cabfbadc2faed6c.
Strike Kimsuky_01d3fc28	This strike sends a malware sample known as Kimsuky. Kimsuky is a malware of the spyware family developed by North Korean groups that targets South Korean think tanks and political entities. It is typically delivered through spear-phishing emails that contain malicious Microsoft Word documents. Once executed, the malware collects information from the infected system and sends it back to the attacker's command-and-control server. The key capabilities of Kimsuky include keystroke logging, capturing screenshots, and stealing documents from the infected system. The MD5 hash of this Kimsuky sample is 01d3fc28e052efaa475727d2b759b51f.
Strike Kimsuky_33d48adb	This strike sends a malware sample known as Kimsuky. Kimsuky is a malware of the spyware family developed by North Korean groups that targets South Korean think tanks and political entities. It is typically delivered through spear-phishing emails that contain malicious Microsoft Word documents. Once executed, the malware collects information from the infected system and sends it back to the attacker's command-and-control server. The key capabilities of Kimsuky include keystroke logging, capturing screenshots, and stealing documents from the infected system. The MD5 hash of this Kimsuky sample is 33d48adb6e36de40185eee6a649274a0.
Strike Kimsuky_349de8d6	This strike sends a malware sample known as Kimsuky. Kimsuky is a malware of the spyware family developed by North Korean groups that targets South Korean think tanks and political entities. It is typically delivered through spear-phishing emails that contain malicious Microsoft Word documents. Once executed, the malware collects information from the infected system and sends it back to the attacker's command-and-control server. The key capabilities of Kimsuky include keystroke logging, capturing screenshots, and stealing documents from the infected system. The MD5 hash of this Kimsuky sample is 349de8d66501b53a38beca5b331d98e5.
Strike Kimsuky_59d11524	This strike sends a malware sample known as Kimsuky. Kimsuky is a malware of the spyware family developed by North Korean groups that targets South Korean think tanks and political entities. It is typically delivered through spear-phishing emails that contain malicious Microsoft Word documents. Once executed, the malware collects information from the infected system and sends it back to the attacker's command-and-control server. The key capabilities of Kimsuky include keystroke logging, capturing screenshots, and stealing documents from the infected system. The MD5 hash of this Kimsuky sample is 59d1152449a503665f552cba0455f02d.
Strike Kimsuky_a8269069	This strike sends a malware sample known as Kimsuky. Kimsuky is a malware of the spyware family developed by North Korean groups that targets South Korean think tanks and political entities. It is typically delivered through spear-phishing emails that contain malicious Microsoft Word documents. Once executed, the malware collects information from the infected system and sends it back to the attacker's command-and-control server. The key capabilities of Kimsuky include keystroke logging, capturing screenshots, and stealing documents from the infected system. The MD5 hash of this Kimsuky sample is a8269069133ecf1924db2b5d712f33ad.

<b>Name</b>	<b>Description</b>
Strike Kimsuky_efee226c	This strike sends a malware sample known as Kimsuky. Kimsuky is a malware of the spyware family developed by North Korean groups that targets South Korean think tanks and political entities. It is typically delivered through spear-phishing emails that contain malicious Microsoft Word documents. Once executed, the malware collects information from the infected system and sends it back to the attacker's command-and-control server. The key capabilities of Kimsuky include keystroke logging, capturing screenshots, and stealing documents from the infected system. The MD5 hash of this Kimsuky sample is efee226c8dc22cc3090709202b853970.
Strike Klopatra_26e59fbf	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is 26e59fbfa6bedc8910638c44986cf8f4.
Strike Klopatra_34ced080	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is 34ced080497311f03e7e5e8ef01b0db3.
Strike Klopatra_4ef93b8b	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is 4ef93b8bb360b87958b8e1f70c0438b8.
Strike Klopatra_7d55b181	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is 7d55b1815aae99cab061fbfd1908e87.

<b>Name</b>	<b>Description</b>
Strike Klopatra_7eb52c6f	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is 7eb52c6f4fd646190b2ba518226a4cdd.
Strike Klopatra_7fe5950a	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is 7fe5950ad2772ac64363e952022a49a5.
Strike Klopatra_ac55f4e3	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is ac55f4e37bb097892100ea25f6dae3cf.
Strike Klopatra_b5988fbc	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is b5988fbce2365e62803a613508070780.
Strike Klopatra_ce73486e	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is ce73486ef665a71f882489e68f842a40.

<b>Name</b>	<b>Description</b>
Strike Klopatra_d553a2db	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is d553a2dbd3076c45008ce4009dff8b97.
Strike Klopatra_d606d84e	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is d606d84eff5f24502204ef5a86af0319.
Strike Klopatra_f8e6ce9e	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is f8e6ce9e7d1749c8f7712ff7c5e16b62.
Strike Klopatra_fa1d6028	This strike sends a malware sample known as Klopatra. Klopatra is a new Android banking Trojan that targets users in Turkey and other countries. It is distributed through third-party application stores and phishing SMS messages that trick users into downloading the malware. Once installed, Klopatra displays a fake login screen to capture banking credentials and sends them to a remote server. The key capabilities of this Trojan include screen overlay attacks, data exfiltration, and remote control of the infected device. The MD5 hash of this Klopatra sample is fa1d6028d68b1d117438915edcb178f8.
Strike Knot_0436580f	This strike sends a polymorphic malware sample known as Knot. Knot is a ransomware that downloads key data to "d.jpg" in the %TEMP%. It requests a ransom to be paid in bitcoin and supplies a knodecryptor once paid to decrypt the user's files. The binary has the checksum removed in the PE file format. The MD5 hash of this Knot sample is 0436580f7e118a3062450ffd13288c02.
Strike Knot_302b61cc	This strike sends a polymorphic malware sample known as Knot. Knot is a ransomware that downloads key data to "d.jpg" in the %TEMP%. It requests a ransom to be paid in bitcoin and supplies a knodecryptor once paid to decrypt the user's files. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Knot sample is 302b61cc09ad102f5b1c05574d91579b.

<b>Name</b>	<b>Description</b>
Strike Knot_5e9dcfb6	This strike sends a malware sample known as Knot. Knot is a ransomware that downloads key data to "d.jpg" in the %TEMP%. It requests a ransom to be paid in bitcoin and supplies a knodecryptor once paid to decrypt the user's files. The MD5 hash of this Knot sample is 5e9dcfb6141d521b6f2b16ab0dbe237e.
Strike Knot_b26cbc5c	This strike sends a polymorphic malware sample known as Knot. Knot is a ransomware that downloads key data to "d.jpg" in the %TEMP%. It requests a ransom to be paid in bitcoin and supplies a knodecryptor once paid to decrypt the user's files. The binary has random bytes appended at the end of the file. The MD5 hash of this Knot sample is b26cbc5c13740cc38a8514e3db80ba49.
Strike Knot_db44127c	This strike sends a polymorphic malware sample known as Knot. Knot is a ransomware that downloads key data to "d.jpg" in the %TEMP%. It requests a ransom to be paid in bitcoin and supplies a knodecryptor once paid to decrypt the user's files. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Knot sample is db44127c7cdff0469fab4474cdaaa452.
Strike Knot_f5254af2	This strike sends a polymorphic malware sample known as Knot. Knot is a ransomware that downloads key data to "d.jpg" in the %TEMP%. It requests a ransom to be paid in bitcoin and supplies a knodecryptor once paid to decrypt the user's files. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Knot sample is f5254af2e940448221167d674cc11fc0.
Strike Knot_fe2bf4f2	This strike sends a polymorphic malware sample known as Knot. Knot is a ransomware that downloads key data to "d.jpg" in the %TEMP%. It requests a ransom to be paid in bitcoin and supplies a knodecryptor once paid to decrypt the user's files. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Knot sample is fe2bf4f242f5e4f03eb16a4b48126212.
Strike Konni_8ce075e4	This strike sends a malware sample known as Konni. This sample belongs to Konni, an APT group that takes advantage of a harmful Russian-language Word document to spread malware on the impacted systems. Konni APT group is known for its sophisticated cyber-espionage campaigns aimed at data exfiltration. Konni leverages an advanced toolset embedded in a harmful Word document through batch scripts and DLL files. The payload includes a User Account Control (UAC) bypass and encrypted communication with a C2 server, allowing attackers to run privileged commands. The MD5 hash of this Konni sample is 8ce075e44ae4ac67862a5024d997161d.
Strike Konni_b6a9f393	This strike sends a malware sample known as Konni. This sample belongs to Konni, an APT group that takes advantage of a harmful Russian-language Word document to spread malware on the impacted systems. Konni APT group is known for its sophisticated cyber-espionage campaigns aimed at data exfiltration. Konni leverages an advanced toolset embedded in a harmful Word document through batch scripts and DLL files. The payload includes a User Account Control (UAC) bypass and encrypted communication with a C2 server, allowing attackers to run privileged commands. The MD5 hash of this Konni sample is b6a9f3933f734f7822da5e7b520ed79d.

<b>Name</b>	<b>Description</b>
Strike Konni_d3282b4d	<p>This strike sends a malware sample known as Konni. This sample belongs to Konni, an APT group that takes advantage of a harmful Russian-language Word document to spread malware on the impacted systems. Konni APT group is known for its sophisticated cyber-espionage campaigns aimed at data exfiltration. Konni leverages an advanced toolset embedded in a harmful Word document through batch scripts and DLL files. The payload includes a User Account Control (UAC) bypass and encrypted communication with a C2 server, allowing attackers to run privileged commands. The MD5 hash of this Konni sample is d3282b4d3ee029c9cdb6ddbd5749206f.</p>
Strike Konni_d7abeff7	<p>This strike sends a malware sample known as Konni. This sample belongs to Konni, an APT group that takes advantage of a harmful Russian-language Word document to spread malware on the impacted systems. Konni APT group is known for its sophisticated cyber-espionage campaigns aimed at data exfiltration. Konni leverages an advanced toolset embedded in a harmful Word document through batch scripts and DLL files. The payload includes a User Account Control (UAC) bypass and encrypted communication with a C2 server, allowing attackers to run privileged commands. The MD5 hash of this Konni sample is d7abeff71b7c6da1954a359d76752b02.</p>
Strike Konni_ed3a7339	<p>This strike sends a malware sample known as Konni. This sample belongs to Konni, an APT group that takes advantage of a harmful Russian-language Word document to spread malware on the impacted systems. Konni APT group is known for its sophisticated cyber-espionage campaigns aimed at data exfiltration. Konni leverages an advanced toolset embedded in a harmful Word document through batch scripts and DLL files. The payload includes a User Account Control (UAC) bypass and encrypted communication with a C2 server, allowing attackers to run privileged commands. The MD5 hash of this Konni sample is ed3a733935eb4c715eb4df1c69473355.</p>
Strike Konni_ffd5de9b	<p>This strike sends a malware sample known as Konni. This sample belongs to Konni, an APT group that takes advantage of a harmful Russian-language Word document to spread malware on the impacted systems. Konni APT group is known for its sophisticated cyber-espionage campaigns aimed at data exfiltration. Konni leverages an advanced toolset embedded in a harmful Word document through batch scripts and DLL files. The payload includes a User Account Control (UAC) bypass and encrypted communication with a C2 server, allowing attackers to run privileged commands. The MD5 hash of this Konni sample is ffd5de9b1e42e07a96299f7242589c08.</p>
Strike Korplug Loader_5e21fab6	<p>This strike sends a malware sample known as Korplug Loader. MQsTTang is malware backdoor that has been attributed to the Mustang Panda APT group. This group has focused primarily on political organizations in Europe and Asia. The Mustang Panda group uses phishing emails to distribute the malware and Github to host the payloads. Once executed the malware duplicates itself and begins enabling persistence by creating a registry key. The malware communicates to the C2 server via the MQTT protocol and includes functionality to detect debugging and monitoring tools in order to evade detection. This file is the Korplug malware loader that has been associated with Mustang Panda and MQsTTang. The MD5 hash of this Korplug Loader sample is 5e21fab62fe16cba1f74e103af13a2db.</p>

<b>Name</b>	<b>Description</b>
Strike Korplug Loader_80bf3ef6	<p>This strike sends a malware sample known as Korplug Loader. MQsTTang is malware backdoor that has been attributed to the Mustang Panda APT group. This group has focused primarily on political organizations in Europe and Asia. The Mustang Panda group uses phishing emails to distribute the malware and Github to host the payloads. Once executed the malware duplicates itself and begins enabling persistence by creating a registry key. The malware communicates to the C2 server via the MQTT protocol and includes functionality to detect debugging and monitoring tools in order to evade detection. This file is the Korplug malware loader that has been associated with Mustang Panda and MQsTTang. The MD5 hash of this Korplug Loader sample is 80bf3ef68826d3472ecbbf1abcb530aa.</p>
Strike Korplug Loader_92170b66	<p>This strike sends a malware sample known as Korplug Loader. MQsTTang is malware backdoor that has been attributed to the Mustang Panda APT group. This group has focused primarily on political organizations in Europe and Asia. The Mustang Panda group uses phishing emails to distribute the malware and Github to host the payloads. Once executed the malware duplicates itself and begins enabling persistence by creating a registry key. The malware communicates to the C2 server via the MQTT protocol and includes functionality to detect debugging and monitoring tools in order to evade detection. This file is the Korplug malware loader that has been associated with Mustang Panda and MQsTTang. The MD5 hash of this Korplug Loader sample is 92170b6635fca111f61d3cf1f35639f0.</p>
Strike Korplug Loader_b1756033	<p>This strike sends a malware sample known as Korplug Loader. MQsTTang is malware backdoor that has been attributed to the Mustang Panda APT group. This group has focused primarily on political organizations in Europe and Asia. The Mustang Panda group uses phishing emails to distribute the malware and Github to host the payloads. Once executed the malware duplicates itself and begins enabling persistence by creating a registry key. The malware communicates to the C2 server via the MQTT protocol and includes functionality to detect debugging and monitoring tools in order to evade detection. This file is the Korplug malware loader that has been associated with Mustang Panda and MQsTTang. The MD5 hash of this Korplug Loader sample is b17560333be41ad41305052e5c52e4eb.</p>
Strike Korplug Loader_d9165591	<p>This strike sends a malware sample known as Korplug Loader. MQsTTang is malware backdoor that has been attributed to the Mustang Panda APT group. This group has focused primarily on political organizations in Europe and Asia. The Mustang Panda group uses phishing emails to distribute the malware and Github to host the payloads. Once executed the malware duplicates itself and begins enabling persistence by creating a registry key. The malware communicates to the C2 server via the MQTT protocol and includes functionality to detect debugging and monitoring tools in order to evade detection. This file is the Korplug malware loader that has been associated with Mustang Panda and MQsTTang. The MD5 hash of this Korplug Loader sample is d91655915849a6451b54a1c7a4aba8b4.</p>
Strike Kryptina_120c6ddf	<p>This strike sends a malware sample known as Kryptina. Kryptina is a Ransomaware-as-a-Service malware written for the Linux platform. It has the ability to automate payloads and manage the groups and ransom payments. The MD5 hash of this Kryptina sample is 120c6ddfc24274b6e2e3a1ba7dc519ab.</p>

<b>Name</b>	<b>Description</b>
Strike Kryptina_1b4bbc6a	This strike sends a malware sample known as Kryptina. Kryptina is a Ransomaware-as-a-Service malware written for the Linux platform. It has the ability to automate payloads and manage the groups and ransom payments. The MD5 hash of this Kryptina sample is 1b4bbc6a2cfe628395c5d670d5ef470d.
Strike Kryptina_231478ff	This strike sends a malware sample known as Kryptina. Kryptina is a Ransomaware-as-a-Service malware written for the Linux platform. It has the ability to automate payloads and manage the groups and ransom payments. The MD5 hash of this Kryptina sample is 231478ff24055d5cdb5fbec36060c8ff.
Strike Kryptina_255796e4	This strike sends a malware sample known as Kryptina. Kryptina is a Ransomaware-as-a-Service malware written for the Linux platform. It has the ability to automate payloads and manage the groups and ransom payments. The MD5 hash of this Kryptina sample is 255796e447b92ece07f2a44f80bd75a6.
Strike Kryptina_45328032	This strike sends a malware sample known as Kryptina. Kryptina is a Ransomaware-as-a-Service malware written for the Linux platform. It has the ability to automate payloads and manage the groups and ransom payments. The MD5 hash of this Kryptina sample is 4532803225b8b1a8a7811a44f3f2e2e6.
Strike Kryptina_66bb9363	This strike sends a malware sample known as Kryptina. Kryptina is a Ransomaware-as-a-Service malware written for the Linux platform. It has the ability to automate payloads and manage the groups and ransom payments. The MD5 hash of this Kryptina sample is 66bb9363e23c7ef2d16c89cd654b491e.
Strike Kryptina_71efe7a2	This strike sends a malware sample known as Kryptina. Kryptina is a Ransomaware-as-a-Service malware written for the Linux platform. It has the ability to automate payloads and manage the groups and ransom payments. The MD5 hash of this Kryptina sample is 71efe7a21da183c407682261612afc0f.
Strike Kryptina_779aa15c	This strike sends a malware sample known as Kryptina. Kryptina is a Ransomaware-as-a-Service malware written for the Linux platform. It has the ability to automate payloads and manage the groups and ransom payments. The MD5 hash of this Kryptina sample is 779aa15cd6a8d416e7f722331d87f47b.
Strike Kryptina_846bb4f2	This strike sends a malware sample known as Kryptina. Kryptina is a Ransomaware-as-a-Service malware written for the Linux platform. It has the ability to automate payloads and manage the groups and ransom payments. The MD5 hash of this Kryptina sample is 846bb4f2cdbf9ed624ba2647c6b04101.
Strike Kryptina_b5b20e03	This strike sends a malware sample known as Kryptina. Kryptina is a Ransomaware-as-a-Service malware written for the Linux platform. It has the ability to automate payloads and manage the groups and ransom payments. The MD5 hash of this Kryptina sample is b5b20e03ae941e9f21c444bd50225c41.
Strike Kryptina_d201bd19	This strike sends a malware sample known as Kryptina. Kryptina is a Ransomaware-as-a-Service malware written for the Linux platform. It has the ability to automate payloads and manage the groups and ransom payments. The MD5 hash of this Kryptina sample is d201bd19e60d500963aff0c235b07727.

<b>Name</b>	<b>Description</b>
Strike Kryptina_fabcc642	This strike sends a malware sample known as Kryptina. Kryptina is a Ransomware-as-a-Service malware written for the Linux platform. It has the ability to automate payloads and manage the groups and ransom payments. The MD5 hash of this Kryptina sample is fabcc64299ec88bcf2815b6c328bdf5e.
Strike KryptoCibule_3165d2f5	This strike sends a malware sample known as KryptoCibule. KryptoCibule is a new malware family that uses the victim resources to mine coins. It tries to hijack transactions by replacing wallet addresses in the clipboard, and exfiltrates cryptocurrency-related files, all while deploying multiple techniques to avoid detection. The MD5 hash of this KryptoCibule sample is 3165d2f5d802226b0dd8d3ccc8336110.
Strike KryptoCibule_437d1461	This strike sends a malware sample known as KryptoCibule. KryptoCibule is a new malware family that uses the victim resources to mine coins. It tries to hijack transactions by replacing wallet addresses in the clipboard, and exfiltrates cryptocurrency-related files, all while deploying multiple techniques to avoid detection. The MD5 hash of this KryptoCibule sample is 437d14610738f18977cefaac1af84686.
Strike KryptoCibule_47a12663	This strike sends a malware sample known as KryptoCibule. KryptoCibule is a new malware family that uses the victim resources to mine coins. It tries to hijack transactions by replacing wallet addresses in the clipboard, and exfiltrates cryptocurrency-related files, all while deploying multiple techniques to avoid detection. The MD5 hash of this KryptoCibule sample is 47a12663fce9b7ad2238f768ba482f49.
Strike Kuiper_0608c64c	This strike sends a malware sample known as Kuiper. Kuiper is a Golang-based ransomware that is advertised for sale in the form of a Ransomware-as-a-Service. It comes in variants supporting different platforms including Windows, Linux and macOS. The malware encrypts user files and appends .kuiper extension to them. Depending on the variant further capabilities of the ransomware include change of the desktop wallpaper, deletion of the malware binaries post-encryption, terminating of selected system processes or removal of volume shadow copies, among others. The MD5 hash of this Kuiper sample is 0608c64c57dcc09246be00f0b2767e6e.
Strike Kuiper_0bfe64b8	This strike sends a malware sample known as Kuiper. Kuiper is a Golang-based ransomware that is advertised for sale in the form of a Ransomware-as-a-Service. It comes in variants supporting different platforms including Windows, Linux and macOS. The malware encrypts user files and appends .kuiper extension to them. Depending on the variant further capabilities of the ransomware include change of the desktop wallpaper, deletion of the malware binaries post-encryption, terminating of selected system processes or removal of volume shadow copies, among others. The MD5 hash of this Kuiper sample is 0bfe64b866911620f273a1d306984d29.
Strike Kuiper_56cabcf9	This strike sends a malware sample known as Kuiper. Kuiper is a Golang-based ransomware that is advertised for sale in the form of a Ransomware-as-a-Service. It comes in variants supporting different platforms including Windows, Linux and macOS. The malware encrypts user files and appends .kuiper extension to them. Depending on the variant further capabilities of the ransomware include change of the desktop wallpaper, deletion of the malware binaries post-encryption, terminating of selected system processes or removal of volume shadow copies, among others. The MD5 hash of this Kuiper sample is 56cabcf95add39a6feb09391ccc40dcd.

<b>Name</b>	<b>Description</b>
Strike Kuiper_84820f3e	This strike sends a malware sample known as Kuiper. Kuiper is a Golang-based ransomware that is advertised for sale in the form of a Ransomware-as-a-Service. It comes in variants supporting different platforms including Windows, Linux and macOS. The malware encrypts user files and appends .kuiper extension to them. Depending on the variant further capabilities of the ransomware include change of the desktop wallpaper, deletion of the malware binaries post-encryption, terminating of selected system processes or removal of volume shadow copies, among others. The MD5 hash of this Kuiper sample is 84820f3eb491a2fde1f52435cd29646c.
Strike Kuiper_8c3c50ec	This strike sends a malware sample known as Kuiper. Kuiper is a Golang-based ransomware that is advertised for sale in the form of a Ransomware-as-a-Service. It comes in variants supporting different platforms including Windows, Linux and macOS. The malware encrypts user files and appends .kuiper extension to them. Depending on the variant further capabilities of the ransomware include change of the desktop wallpaper, deletion of the malware binaries post-encryption, terminating of selected system processes or removal of volume shadow copies, among others. The MD5 hash of this Kuiper sample is 8c3c50ecee8744ad77a517ed39a25880.
Strike Kuluoz_027c9e37	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 027c9e37727eb43750c927fda422ca5d.
Strike Kuluoz_031fce2f	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has a new section added in the PE file format with random contents. The MD5 hash of this Kuluoz sample is 031fce2f46862d4bd7055da4333cfa66.
Strike Kuluoz_039cff92	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 039cff9230fcffba3694edf15ae0a6d9.
Strike Kuluoz_0616f3c9	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Kuluoz sample is 0616f3c930b80fb8ed66810c2ea97fc.
Strike Kuluoz_070529b2	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 070529b2be131b5a260ed9df6583122e.
Strike Kuluoz_07225812	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 07225812ff73655b7151ddb5585a383c.

<b>Name</b>	<b>Description</b>
Strike Kuluo_082721c6	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 082721c6a65a2e6f1c9c16db10f5ab9c.
Strike Kuluo_08a5665e	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random bytes appended at the end of the file. The MD5 hash of this Kuluo sample is 08a5665e588077e5ee093952d7dfffc1c.
Strike Kuluo_0b0061e5	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Kuluo sample is 0b0061e58c3626c7a01b5e02c1c46240.
Strike Kuluo_0fec7e00	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 0fec7e00c7c25b6100c1486bdccc90ae.
Strike Kuluo_11c108f7	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Kuluo sample is 11c108f7a7e10c3b8c83b4822bc10a30.
Strike Kuluo_13186602	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 1318660229c3303b7ca6cc790116c376.
Strike Kuluo_1351ebf2	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has been packed using upx packer, with the default options. The MD5 hash of this Kuluo sample is 1351ebf2a8b179fb456dc70bc87e891.
Strike Kuluo_14d35354	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Kuluo sample is 14d35354a20f9a516b7225b6372b3af5.
Strike Kuluo_15eea0b0	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 15eea0b06b959593fd357c976a98c824.

<b>Name</b>	<b>Description</b>
Strike Kuluo_17409590	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Kuluoz sample is 174095907aeaffda652d87c33bc6899f.
Strike Kuluo_18ebe58a	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 18ebe58a606b06daac837db615ceb3ae.
Strike Kuluo_19244e86	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary file has one more imports added in the import table. The MD5 hash of this Kuluoz sample is 19244e8666f85a39f977c878d4ca17e7.
Strike Kuluo_1ad639e3	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Kuluoz sample is 1ad639e3f520caef6fb25628e9676cca.
Strike Kuluo_1d0da87d	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 1d0da87d04a68d52f9474a50e324e3af.
Strike Kuluo_1d5c1d91	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 1d5c1d91765a64808c6ee8452b3ad55e.
Strike Kuluo_1f26d68a	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 1f26d68a92fc1c144bc6297e982eba37.
Strike Kuluo_1fbc4166	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 1fbc41665b81361d63232240850517e9.
Strike Kuluo_20aa747f	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 20aa747fa92e691e0e46e09bcf7a83c3.
Strike Kuluo_22f7171e	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 22f7171ebb630b38cbfc288ccfea9b91.

<b>Name</b>	<b>Description</b>
Strike Kuluo_22fbf3b7	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Kuluo sample is 22fbf3b79f80ab0ee9850316a402fa58.
Strike Kuluo_2470172c	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 2470172c7e9f2ead84917c01bb009992.
Strike Kuluo_287f6409	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 287f6409bcd54c59c175fce1abb995.
Strike Kuluo_291eb74d	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 291eb74d506802c09985eefcd7b55f43.
Strike Kuluo_29ff333d	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 29ff333df9b82790a19b06bce2696586.
Strike Kuluo_2affda67	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 2affda6728c1e7df9c897ae43f7e4847.
Strike Kuluo_2ebfec62	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 2ebfec626dce31ca659db6d32b3baabc.
Strike Kuluo_2f1e72c7	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 2f1e72c7c360157a2842eda8663cae52.
Strike Kuluo_317767f7	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 317767f77668bbd3f31cf19b7c0fb99.
Strike Kuluo_330ba1d3	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has the checksum removed in the PE file format. The MD5 hash of this Kuluo sample is 330ba1d383004c9ca6dca37fbbea2467.

<b>Name</b>	<b>Description</b>
Strike Kuluo_351a9389	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 351a938965339a71b890c26f163da37f.
Strike Kuluo_3531fecd	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 3531fecd47a9757aaa8ec5015380e0fe.
Strike Kuluo_36b27d3c	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Kuluo sample is 36b27d3cbb0ff0a08c92098a6f2fa708.
Strike Kuluo_3d2be4f6	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 3d2be4f6be65738d71e6f84c737d4f59.
Strike Kuluo_3e015bab	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 3e015bab445cb8763636cd4a4c66d801.
Strike Kuluo_40f9503f	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 40f9503fcdbb866cd1492c494b32c411.
Strike Kuluo_426e964b	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 426e964b0e2d38ea23e9f88093069c67.
Strike Kuluo_4460d964	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 4460d9646883add6b268e0bbf24f1fe7.
Strike Kuluo_44786ada	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random bytes appended at the end of the file. The MD5 hash of this Kuluo sample is 44786adad78ace8126e62d0db2d926c1.
Strike Kuluo_4590a340	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Kuluo sample is 4590a3401e47f5c6aec094babfff788a.

<b>Name</b>	<b>Description</b>
Strike Kuluo_46145172	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 46145172a29febe6003f167759b1bc56.
Strike Kuluo_4733d52f	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 4733d52f96bdd83e37b69ead8711d961.
Strike Kuluo_488189b3	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 488189b39be082a52ebf3e9392d12f34.
Strike Kuluo_4899bfe8	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 4899bfe897bf03d2a59beac556f29c5.
Strike Kuluo_48cdcf41	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 48cdcf4163aed13475782b1fc644727b.
Strike Kuluo_4b0b0ee7	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 4b0b0ee76f1ec24fe43fe8465d435b8f.
Strike Kuluo_4d652077	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 4d6520775f6625f851647fa3b747743c.
Strike Kuluo_4e33b0d1	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 4e33b0d1758bd93b08eea3da59dc068e.
Strike Kuluo_4e8e554f	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary file has one more imports added in the import table. The MD5 hash of this Kuluo sample is 4e8e554f7497518fa5a84e48ae5af670.
Strike Kuluo_4f2d6b2a	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary file has one more imports added in the import table. The MD5 hash of this Kuluo sample is 4f2d6b2ad873d6e30155a0dd44202d55.

<b>Name</b>	<b>Description</b>
Strike Kuluo_4f51e417	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 4f51e417e45c7d9a5f1cbd4198b93f96.
Strike Kuluo_5046f352	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Kuluo sample is 5046f3525d1bc14cabd3abae9ea0eb7c.
Strike Kuluo_52cc3435	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 52cc34357dd39b32c6f2ebbefa472986.
Strike Kuluo_542db33b	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 542db33b01da6eea559144d6e671fa4e.
Strike Kuluo_551b07af	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary file has one more imports added in the import table. The MD5 hash of this Kuluo sample is 551b07af1f1a2ce681c488b401625faf.
Strike Kuluo_5afe943a	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Kuluo sample is 5afe943a3fde584fcf5fed55ce5b1d79.
Strike Kuluo_5c58a9fb	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Kuluo sample is 5c58a9fbfc602a77c755b950790a8012.
Strike Kuluo_5d11db15	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has been packed using upx packer, with the default options. The MD5 hash of this Kuluo sample is 5d11db1549292bf2c44d253a1dfd3e18.
Strike Kuluo_600b87cf	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 600b87cfcb2352e0710a32ab9787d9f5.

<b>Name</b>	<b>Description</b>
Strike Kuluoz_6302a1e7	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 6302a1e74ad439abe9f38f2d28ff846d.
Strike Kuluoz_639147d6	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 639147d6eae567f8d88715bef315905c.
Strike Kuluoz_65d19829	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 65d19829875f1513eea13f0bbe2947c8.
Strike Kuluoz_678fa6d7	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 678fa6d7254b0ab4ed2f895256f03c17.
Strike Kuluoz_681b9704	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 681b97043169c2431ddbbe457e3ab85d.
Strike Kuluoz_68dfa31b	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random bytes appended at the end of the file. The MD5 hash of this Kuluoz sample is 68dfa31bf8c4a2056cff7f037396a21f.
Strike Kuluoz_6aa2aab7	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 6aa2aab7d3b701812b6515644d2598d0.
Strike Kuluoz_6b3de80c	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has been packed using upx packer, with the default options. The MD5 hash of this Kuluoz sample is 6b3de80c056c5ce27414a16f1b3e0c8b.
Strike Kuluoz_6c605ebf	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 6c605ebf5c50898355ad69027897198f.
Strike Kuluoz_6fdd6663	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 6fdd666304034cb79543a52aac70f787.

<b>Name</b>	<b>Description</b>
Strike Kuluoz_723dc107	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 723dc107a8b1ac080ea3e5ac641dbc68.
Strike Kuluoz_7539c94b	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 7539c94b87c2f141589181e77b57d6b5.
Strike Kuluoz_770e42fa	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 770e42fa612a899ed1c87a5b46cc466f.
Strike Kuluoz_77aca864	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 77aca864bb43d404baa9ecfb97d130d.
Strike Kuluoz_77e14aca	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has been packed using upx packer, with the default options. The MD5 hash of this Kuluoz sample is 77e14aca659a6bd06a52e0faad013826.
Strike Kuluoz_78377e36	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Kuluoz sample is 78377e36b6339a170a5c7a9c38c0fc09.
Strike Kuluoz_7d34c334	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 7d34c334b27aa770df9ea753945cb4fb.
Strike Kuluoz_7d75d555	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Kuluoz sample is 7d75d555f3490789f7a9a129e4c34d26.
Strike Kuluoz_82e0eb26	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 82e0eb2601aaed8c2c86905f4011a68a.
Strike Kuluoz_838f9a5e	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is 838f9a5eac96fce37f3ba5de28ba5d81.

<b>Name</b>	<b>Description</b>
Strike Kuluo_86631965	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Kuluo sample is 866319652a22b4be324d298aefda62b7.
Strike Kuluo_8c50454c	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 8c50454c2720cd0b8c50aa7977dbc28a.
Strike Kuluo_8f5c3202	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random bytes appended at the end of the file. The MD5 hash of this Kuluo sample is 8f5c320206923f7e06ff383791843518.
Strike Kuluo_93793281	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 937932817fad19389760ab3a9880d0fe.
Strike Kuluo_93af451a	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 93af451a9a9b7ce0b3f227ba2d6ad085.
Strike Kuluo_97765c75	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 97765c75f51e113c6acf427e006d4bb3.
Strike Kuluo_97cb5078	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 97cb5078dd3beed3619d78a1a74cb698.
Strike Kuluo_9849c613	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 9849c613e8add1b4c40dc6e21516809c.
Strike Kuluo_9887fa9e	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is 9887fa9e47fed89b74599c387907b794.
Strike Kuluo_9a15bffa	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has been packed using upx packer, with the default options. The MD5 hash of this Kuluo sample is 9a15bffa27d1ee27dedfe8502aac198e.

<b>Name</b>	<b>Description</b>
Strike Kuluo_9f102a84	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Kuluo sample is 9f102a84f196533b26202fed7c996a25.
Strike Kuluo_a0113745	This strike sends a polymorphic malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary file has one more imports added in the import table. The MD5 hash of this Kuluo sample is a0113745dc6cf9ac1346da1edb91d07a.
Strike Kuluo_a0318efb	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is a0318efb7b883fc4c725bdf72c3ed5f1.
Strike Kuluo_a21740b0	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is a21740b03a097f9323dcf55887e372f4.
Strike Kuluo_a250b5c8	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is a250b5c892d7c5b73d1d37b5305b1898.
Strike Kuluo_a26c6aca	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is a26c6aca229b4012e78497689baac26f.
Strike Kuluo_a2afe5d1	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is a2afe5d161efec64eb761c98bd78a778.
Strike Kuluo_a2d400fe	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is a2d400fec6cc641a1cbe40e3eda7033.
Strike Kuluo_a6584ff4	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is a6584ff407513e6bb84599908b01b78a.
Strike Kuluo_a7d2ae19	This strike sends a malware sample known as Kuluo. Kuluo also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo sample is a7d2ae192489f6494346f91efb1bfe83.

<b>Name</b>	<b>Description</b>
Strike Kuluo_z_a7e29d98	This strike sends a polymorphic malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary file has one more imports added in the import table. The MD5 hash of this Kuluo_z sample is a7e29d98e9bb31285477a9790346f9f4.
Strike Kuluo_z_a8376144	This strike sends a polymorphic malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has been packed using upx packer, with the default options. The MD5 hash of this Kuluo_z sample is a8376144472b76b3df8c4ab2aa626511.
Strike Kuluo_z_a84de6a0	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is a84de6a0384f75f5e465250a552d8fa0.
Strike Kuluo_z_adf212a0	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is adf212a0e7d0cc067e27bff1d6ecad3b.
Strike Kuluo_z_af04de71	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is af04de71b83c9154f0fa96dee30af38c.
Strike Kuluo_z_b23f52f9	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is b23f52f94d56fca439a4ec7f9de8c496.
Strike Kuluo_z_b3bb969a	This strike sends a polymorphic malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Kuluo_z sample is b3bb969a3fc26077a914f6d2c558cdb5.
Strike Kuluo_z_b48e028e	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is b48e028e2c22b329aa4b3308c95a1963.
Strike Kuluo_z_b65935d5	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is b65935d5de9514b4b1e67bff182f503f.
Strike Kuluo_z_b97fe5e4	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is b97fe5e4dda43c145fd578d0553286c6.

<b>Name</b>	<b>Description</b>
Strike Kuluo_z_bbf64157	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is bbf641577091d3372fa3ef072fc1c9d5.
Strike Kuluo_z_c161c8e6	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is c161c8e6526a950c5f357315bd7e42c0.
Strike Kuluo_z_c21c9212	This strike sends a polymorphic malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Kuluo_z sample is c21c92123b7ac18638fa07dcdd29551d.
Strike Kuluo_z_c52ddca0	This strike sends a polymorphic malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random bytes appended at the end of the file. The MD5 hash of this Kuluo_z sample is c52ddca0b8d70c58ae15dfa151d023c4.
Strike Kuluo_z_c5ac8863	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is c5ac8863efddb0bc1dc7781353a4ac06.
Strike Kuluo_z_c68b0470	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is c68b0470a04ba3eb2a42ebe8bf04f9ae.
Strike Kuluo_z_c6f79921	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is c6f7992199f83d089e6c108b6b0896ff.
Strike Kuluo_z_c806314b	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is c806314b2408d24675193f8d57ea13c5.
Strike Kuluo_z_c8984053	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is c8984053c52f9c5aa349cc2023d482bb.
Strike Kuluo_z_c90925bd	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is c90925bd4346ed71a973b82f63aae70f.

<b>Name</b>	<b>Description</b>
Strike Kuluo_z_cd4ac536	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Kuluoz sample is cd4ac536df9094ae4ce7a01bbc63db75.
Strike Kuluo_z_cdf5509f	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is cdf5509f6620ea3199e5bd0a34530435.
Strike Kuluo_z_ce5d9471	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is ce5d9471ef2eb0a7af34c71b55a74ed6.
Strike Kuluo_z_cec71cb6	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Kuluoz sample is cec71cb6ee95b5faf0e7a1fe3e1fe865.
Strike Kuluo_z_d0c01d3e	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is d0c01d3eb5f3b48ca331f9936460f887.
Strike Kuluo_z_d78697f6	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is d78697f62bbc18e4623fc6265668673c.
Strike Kuluo_z_d78b0fd6	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is d78b0fd6e3905e5572f086ab32f78946.
Strike Kuluo_z_d9d39de7	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Kuluoz sample is d9d39de7633887b6185c62226823be47.
Strike Kuluo_z_db2009d7	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is db2009d7c82036c0f342cb14121a132f.

<b>Name</b>	<b>Description</b>
Strike Kuluo_z_db75c1d3	This strike sends a polymorphic malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Kuluo_z sample is db75c1d3275504ef331f667fa7d3b79c.
Strike Kuluo_z_dc03588f	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is dc03588f2f3ff5a9797f2ee2e23c1473.
Strike Kuluo_z_e0389d5e	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is e0389d5e1468add772d596c39e3f58c.
Strike Kuluo_z_e38266f7	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is e38266f7609f8a8038cc707ac3981e5b.
Strike Kuluo_z_e41c6689	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is e41c66894d11d3cf4f599785ab6b554b.
Strike Kuluo_z_e492fc18	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is e492fc1829fdd76ba7a8a0092f0a8b2a.
Strike Kuluo_z_e4c1130b	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is e4c1130b2e0c2b07ddd4ff633be95408.
Strike Kuluo_z_e5e03f8f	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is e5e03f8fe42271ebe1c3f93d223cd726.
Strike Kuluo_z_e76477e1	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is e76477e155e9b21069f8c7dfb2722cfc.
Strike Kuluo_z_e9431443	This strike sends a malware sample known as Kuluo_z. Kuluo_z also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluo_z sample is e9431443b0061f5e1ed3ca59bf265c23.

<b>Name</b>	<b>Description</b>
Strike Kuluoz_ea87a054	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is ea87a054f0f61ca41781c4a428d90070.
Strike Kuluoz_f1ac4923	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is f1ac4923d1e326a32f3036cdf8d16509.
Strike Kuluoz_f328c1a0	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is f328c1a0ab5d0bd50d346ffe5e4dcc5f.
Strike Kuluoz_f3f4fb94	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random bytes appended at the end of the file. The MD5 hash of this Kuluoz sample is f3f4fb94b96c123a321d122c90b3380c.
Strike Kuluoz_f432f364	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is f432f364ce5519eaf929f949696467fc.
Strike Kuluoz_f777c82e	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is f777c82e0d45432bef27b57baa74dc48.
Strike Kuluoz_f7e2deea	This strike sends a polymorphic malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Kuluoz sample is f7e2deea538a9efb9e03f2c7750a94f8.
Strike Kuluoz_f818a873	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is f818a8731476ae4471e348d2b6ecd94.
Strike Kuluoz_fe82f4f2	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is fe82f4f2854df62c607a4a2a2e053e79.
Strike Kuluoz_ffdb03de	This strike sends a malware sample known as Kuluoz. Kuluoz also called Asprox is a remote access trojan that has been known to download and execute additional malware like fake antivirus software. The MD5 hash of this Kuluoz sample is ffdb03defeb3b3edabae49fc1b0c360d.

<b>Name</b>	<b>Description</b>
Strike LATENTBOT_08bb5f82	This strike sends a malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The MD5 hash of this LATENTBOT sample is 08bb5f82dec4957ad9da12239f606a00.
Strike LATENTBOT_1dd0854a	This strike sends a malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The MD5 hash of this LATENTBOT sample is 1dd0854a73288e833966fde139ffe385.
Strike LATENTBOT_2aaa53ce	This strike sends a polymorphic malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this LATENTBOT sample is 2aaa53ce895c64e5c1e168f0b2d7ce2f.
Strike LATENTBOT_2d2484d5	This strike sends a malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The MD5 hash of this LATENTBOT sample is 2d2484d578bfcd983acb151c89e5a120.
Strike LATENTBOT_4135552b	This strike sends a malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The MD5 hash of this LATENTBOT sample is 4135552b0045e7d67b26167f43b88a30.
Strike LATENTBOT_47f220f6	This strike sends a malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The MD5 hash of this LATENTBOT sample is 47f220f6110ecba74a69928c20ce9d3e.
Strike LATENTBOT_4d0b1402	This strike sends a malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The MD5 hash of this LATENTBOT sample is 4d0b14024d4a7ffcff25f2a3ce337af8.
Strike LATENTBOT_5446022c	This strike sends a malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The MD5 hash of this LATENTBOT sample is 5446022c6d14a45fd6ef412a2d6601c5.
Strike LATENTBOT_56ba76cf	This strike sends a malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The MD5 hash of this LATENTBOT sample is 56ba76cf35a1121bf83920003c2af825.

<b>Name</b>	<b>Description</b>
Strike LATENTBOT_5eaf2d54	This strike sends a polymorphic malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The binary has the timestamp field updated in the PE file header. The MD5 hash of this LATENTBOT sample is 5eaf2d547323c5bbb89290ae1cbf9ab5.
Strike LATENTBOT_6ea9d27d	This strike sends a malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The MD5 hash of this LATENTBOT sample is 6ea9d27d23646fc94e05b8c5e921db99.
Strike LATENTBOT_a11362a8	This strike sends a malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The MD5 hash of this LATENTBOT sample is a11362a8e32b5641e90920729d61b3d4.
Strike LATENTBOT_af15076a	This strike sends a malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The MD5 hash of this LATENTBOT sample is af15076a22576f270af0111b93fe6e03.
Strike LATENTBOT_d349806e	This strike sends a malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The MD5 hash of this LATENTBOT sample is d349806ea1f2af0f447b2c9e20cb88f0.
Strike LATENTBOT_fa20c7f3	This strike sends a polymorphic malware sample known as LATENTBOT. LATENTBOT is a malware which may be used to harvest credentials, encrypt and ransom an infected target, or wipe the infected hard drive. It has been found in the wild since 2013. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this LATENTBOT sample is fa20c7f3e1091c12dde319acf4b75b9a.
Strike Letscall_e84d00df	This strike sends a malware sample known as Letscall. Letscall is a Voice over IP Phishing malware. The malware is 3 stages in its attack. The first stage prepares the device by acquiring the necessary permissions and then launches a phishing page. The second stage is then downloaded from a C2 server. In the second stage the device is infected with spyware and enlisted in a P2P VOIP network for communication. The third stage of the malware includes many capabilities such as the ability to redirect outbound calls to the attacker controlled call center for further social engineering. The MD5 hash of this Letscall sample is e84d00df86ab5edfc8c26ae89ca0508.
Strike Liberator_5acdd854	This strike sends a polymorphic malware sample known as Liberator. Liberator is malware distributed by the group known as disBalancer as a tool that offers users the ability to perform DDoS attacks against Russian propaganda websites in an effort to help Ukraine. However unknown to users, these files once downloaded infect the system with malware like info-stealers designed to dump credentials and cryptocurrency-related information. The binary has the checksum removed in the PE file format. The MD5 hash of this Liberator sample is 5acdd8541c6085cd0dc03670bb4cf157.

<b>Name</b>	<b>Description</b>
Strike Liberator_5c0693ed	This strike sends a malware sample known as Liberator. Liberator is malware distributed by the group known as disBalancer as a tool that offers users the ability to perform DDoS attacks against Russian propaganda websites in an effort to help Ukraine. However unknown to users, these files once downloaded infect the system with malware like info-stealers designed to dump credentials and cryptocurrency-related information. The MD5 hash of this Liberator sample is 5c0693ed5953c01ccf046b8a9461efa3.
Strike Liberator_62b9e5b4	This strike sends a malware sample known as Liberator. Liberator is malware distributed by the group known as disBalancer as a tool that offers users the ability to perform DDoS attacks against Russian propaganda websites in an effort to help Ukraine. However unknown to users, these files once downloaded infect the system with malware like info-stealers designed to dump credentials and cryptocurrency-related information. The MD5 hash of this Liberator sample is 62b9e5b4b36511838fc8960202a88d45.
Strike Liberator_876b71d3	This strike sends a malware sample known as Liberator. Liberator is malware distributed by the group known as disBalancer as a tool that offers users the ability to perform DDoS attacks against Russian propaganda websites in an effort to help Ukraine. However unknown to users, these files once downloaded infect the system with malware like info-stealers designed to dump credentials and cryptocurrency-related information. The MD5 hash of this Liberator sample is 876b71d32631eb0980cf48e839566204.
Strike Liberator_a177262e	This strike sends a polymorphic malware sample known as Liberator. Liberator is malware distributed by the group known as disBalancer as a tool that offers users the ability to perform DDoS attacks against Russian propaganda websites in an effort to help Ukraine. However unknown to users, these files once downloaded infect the system with malware like info-stealers designed to dump credentials and cryptocurrency-related information. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Liberator sample is a177262efae98183e97bd29357c9aad2.
Strike Liberator_cc720105	This strike sends a polymorphic malware sample known as Liberator. Liberator is malware distributed by the group known as disBalancer as a tool that offers users the ability to perform DDoS attacks against Russian propaganda websites in an effort to help Ukraine. However unknown to users, these files once downloaded infect the system with malware like info-stealers designed to dump credentials and cryptocurrency-related information. The binary has random bytes appended at the end of the file. The MD5 hash of this Liberator sample is cc7201057f28437d8c1d32deb8bcf4b7.
Strike Liberator_d60e2151	This strike sends a polymorphic malware sample known as Liberator. Liberator is malware distributed by the group known as disBalancer as a tool that offers users the ability to perform DDoS attacks against Russian propaganda websites in an effort to help Ukraine. However unknown to users, these files once downloaded infect the system with malware like info-stealers designed to dump credentials and cryptocurrency-related information. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Liberator sample is d60e2151cc438b1c6378d23aedd7f3b1.

<b>Name</b>	<b>Description</b>
Strike Liberator_dd20876b	This strike sends a malware sample known as Liberator. Liberator is malware distributed by the group known as disBalancer as a tool that offers users the ability to perform DDoS attacks against Russian propaganda websites in an effort to help Ukraine. However unknown to users, these files once downloaded infect the system with malware like info-stealers designed to dump credentials and cryptocurrency-related information. The MD5 hash of this Liberator sample is dd20876bf25544aa55e0c3725103c666.
Strike Liberator_ee1b1be4	This strike sends a polymorphic malware sample known as Liberator. Liberator is malware distributed by the group known as disBalancer as a tool that offers users the ability to perform DDoS attacks against Russian propaganda websites in an effort to help Ukraine. However unknown to users, these files once downloaded infect the system with malware like info-stealers designed to dump credentials and cryptocurrency-related information. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Liberator sample is ee1b1be464867edc5e847b3f219ab85b.
Strike Lightrail_0a739dbd	This strike sends a malware sample known as Lightrail. Lightrail is a tunneler that has been associated with the Minibike and Minibus backdoor malware and the UNC1549 threat actor. It uses the Azure cloud infrastructure to communicate with command and control servers. The MD5 hash of this Lightrail sample is 0a739dbdbcf9a5d8389511732371ecb4.
Strike Lightrail_36e2d9ce	This strike sends a malware sample known as Lightrail. Lightrail is a tunneler that has been associated with the Minibike and Minibus backdoor malware and the UNC1549 threat actor. It uses the Azure cloud infrastructure to communicate with command and control servers. The MD5 hash of this Lightrail sample is 36e2d9ce19ed045a9840313439d6f18d.
Strike Lightrail_a5fdf55c	This strike sends a malware sample known as Lightrail. Lightrail is a tunneler that has been associated with the Minibike and Minibus backdoor malware and the UNC1549 threat actor. It uses the Azure cloud infrastructure to communicate with command and control servers. The MD5 hash of this Lightrail sample is a5fdf55c1c50be471946de937f1e46dd.
Strike Lightrail_aaef98be	This strike sends a malware sample known as Lightrail. Lightrail is a tunneler that has been associated with the Minibike and Minibus backdoor malware and the UNC1549 threat actor. It uses the Azure cloud infrastructure to communicate with command and control servers. The MD5 hash of this Lightrail sample is aaef98be8e58be6b96566268c163b6aa.
Strike Lightrail_c3830b13	This strike sends a malware sample known as Lightrail. Lightrail is a tunneler that has been associated with the Minibike and Minibus backdoor malware and the UNC1549 threat actor. It uses the Azure cloud infrastructure to communicate with command and control servers. The MD5 hash of this Lightrail sample is c3830b1381d95aa6f97a58fd8ff3524e.
Strike Lightrail_c51bc86b	This strike sends a malware sample known as Lightrail. Lightrail is a tunneler that has been associated with the Minibike and Minibus backdoor malware and the UNC1549 threat actor. It uses the Azure cloud infrastructure to communicate with command and control servers. The MD5 hash of this Lightrail sample is c51bc86beb9e16d1c905160e96d9fa29.

<b>Name</b>	<b>Description</b>
Strike Linux.Gomir_e562cf30	This strike sends a malware sample known as Linux.Gomir. Linux.Gomir is a Linux backdoor developed by the North Korean group Springtail. Similar to the Windows GoBear backdoor, it communicates with a C2 server to receive encrypted commands to execute. The MD5 hash of this Linux.Gomir sample is e562cf30d17d47347c7e6ffd249fc190.
Strike Lontail_1176381d	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is 1176381da7dea356f3377a59a6f0e799.
Strike Lontail_126bc1c3	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is 126bc1c30fba27f8bf67dce4892b1e8c.
Strike Lontail_16217533	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is 16217533756678968169932c05280d94.
Strike Lontail_2e803d28	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is 2e803d28809be2a0216f25126efde37b.
Strike Lontail_31f2369d	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is 31f2369d2e38c78f5b3f2035dba07c08.

<b>Name</b>	<b>Description</b>
Strike Lontail_3dd829fb	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is 3dd829fb27353622eff34be1eabb8f18.
Strike Lontail_46804472	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is 46804472541ed61cc904cd14be18fe1d.
Strike Lontail_4abcf21b	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is 4abcf21b63781a53bbc1aa17bd8d2cbc.
Strike Lontail_4dd6250e	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is 4dd6250eb2d368f500949952eb013964.
Strike Lontail_57c916da	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is 57c916da83cc634af22bde0ad44d0db3.
Strike Lontail_85427a8a	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is 85427a8a47c4162b48d8dfb37440665d.

<b>Name</b>	<b>Description</b>
Strike Lontail_929b12bc	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is 929b12bc9f9e5f8e854de1d46ebf40d9.
Strike Lontail_a90236e4	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is a90236e4962620949b720f647a91f101.
Strike Lontail_c21eefc6	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is c21eefc65cda49f17ddd1d243a7bffb5.
Strike Lontail_da0085a9	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is da0085a97c38ead734885e5cced1847f.
Strike Lontail_f0dfb7bf	This strike sends a malware sample known as Lontail. Lontail is a sophisticated passive backdoor installed on Windows servers that enables attackers to execute commands remotely through HTTP requests. It targets high-profile organizations in the Middle East, including government, military, telecommunications, and financial institutions. Lontail includes custom loaders and memory-resident shellcode payloads and leverages undocumented features of the HTTP.sys driver for payload extraction. The MD5 hash of this Lontail sample is f0dfb7bf01c0412891da8fa2702f4c7b.
Strike LitterDrifter_1536ec56	This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 1536ec56d69cc7e9aebb8fb0d3277c4.

<b>Name</b>	<b>Description</b>
Strike LitterDrifter_1da0bf90	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 1da0bf901ae15a9a8aef89243516c818.</p>
Strike LitterDrifter_2239800b	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 2239800bfc8fdfddf78229f2eb8a7b95.</p>
Strike LitterDrifter_2996a70d	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 2996a70d09fff69f209051ce75a9b4f8.</p>
Strike LitterDrifter_42bc36d5	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 42bc36d5debc21dff3559870ff300c4e.</p>
Strike LitterDrifter_495b118d	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 495b118d11ceae029d186ffdbb157614.</p>

<b>Name</b>	<b>Description</b>
Strike LitterDrifter_49d1f9ce	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 49d1f9ce1d0f6dfa94ad9b0548384b3a.</p>
Strike LitterDrifter_4c2431e5	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 4c2431e5f868228c1f286fca1033d221.</p>
Strike LitterDrifter_579f1883	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 579f1883cd8534167e773341e27990.</p>
Strike LitterDrifter_6349dd85	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 6349dd85d9549f333117a84946972d06.</p>
Strike LitterDrifter_8096dfaa	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 8096dfaa954113242011e0d7aaaebffd.</p>

<b>Name</b>	<b>Description</b>
Strike LitterDrifter_83500309	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 83500309a878370722bc40c7b83e83e3.</p>
Strike LitterDrifter_86d28664	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 86d28664fc7332eafb788a44ac82a5ed.</p>
Strike LitterDrifter_88aba3f2	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 88aba3f2d526b0ba3db9bc3dfee7db39.</p>
Strike LitterDrifter_96db6240	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 96db6240acb1a3fca8add7c4f9472aa5.</p>
Strike LitterDrifter_9d9851d6	<p>This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is 9d9851d672293dfd8354081fd0263c13.</p>

<b>Name</b>	<b>Description</b>
Strike LitterDrifter_bbb464b3	This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is bbb464b327ad259ad5de7ce3e85a4081.
Strike LitterDrifter_cbeaedfa	This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is cbeaedfa84b02a2bd41a70fa92a46c36.
Strike LitterDrifter_cdae1c55	This strike sends a malware sample known as LitterDrifter. LitterDrifter, associated with Gamaredon, is a USB-propagating worm, written in VBS, that autonomously spreads via USB drives and communicates with a dynamic command-and-control infrastructure. Evolving from a prior Gamaredon USB Powershell worm, LitterDrifter ensures persistent control across diverse global targets. Orchestrated by "trash.dll," it effectively spreads and establishes a resilient command and control channel. The spreader module targets USB removable media, while the C2 module manages communication with the attacker's servers and executes payloads. The MD5 hash of this LitterDrifter sample is cdae1c55ec154cd6cef4954519564c01.
Strike LockBit Black_7e37f198	This strike sends a malware sample known as LockBit Black. The LockBit Black malware variant performs anti-forensic functions like killing multiple tasks, clearing logs and deleting services. It obtains initial access to the victim's network via SMB brute forcing, and uses PSEXEC to execute files and spread laterally across the network. The MD5 hash of this LockBit Black sample is 7e37f198c71a81af5384c480520ee36e.
Strike LockBit_04436f49	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 04436f490b3491218e3793a568484624.
Strike LockBit_06bd47b8	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 06bd47b8ec7e6277dc6c8842d00f7243.

<b>Name</b>	<b>Description</b>
Strike LockBit_0859a78b	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 0859a78bb06a77e7c6758276eafbefd9.
Strike LockBit_089e3b6a	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 089e3b6a539d4c7099cc5fdf559e01e.
Strike LockBit_0d03306e	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 0d03306ed6dd40407e8ae0fa3ffc181f.
Strike LockBit_0e3501b3	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 0e3501b3b6626c98793588b8eca7122e.
Strike LockBit_0f28c0c3	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 0f28c0c3a2d7206816f15111ae7a3141.
Strike LockBit_11d6a53e	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 11d6a53e5ca41ce15b7f09b1c68dcfb1.
Strike LockBit_12351122	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 123511227718f17b3dec5431d5ae87f3.
Strike LockBit_18aff9c4	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 18aff9c4264f6d7e5b0dec5bf944f276.
Strike LockBit_1dbb4f12	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 1dbb4f122e2ccaf5ef2003a827367c34.
Strike LockBit_1f4f6abf	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 1f4f6abfcfd4c347ba951a04c8d86982.

<b>Name</b>	<b>Description</b>
Strike LockBit_1fbef2a9	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 1fbef2a9007eb0e32fb586e0fca3f0e7.
Strike LockBit_207718c9	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 207718c939673a5f674ce51f402fc06.
Strike LockBit_2599bd20	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 2599bd20a5c84309e1c1a80b0041f685.
Strike LockBit_265d02e0	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 265d02e0a563bbdbdb2883add41ff4bb.
Strike LockBit_28afbe8d	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 28afbe8d30dd2950702275bbb611d4cb.
Strike LockBit_306b16a3	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 306b16a367f9d534a976e3ecb6ed5549.
Strike LockBit_37ec80fb	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 37ec80fb2302d5893cb6984cb1a43e2.
Strike LockBit_3826fca4	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 3826fca41ae4c2d799bb6948e2fed18f.
Strike LockBit_3fa216f0	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 3fa216f058ffdlda8f15ba47d5ff07e1.
Strike LockBit_43b1b8cf	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 43b1b8cf880ce5c904b9da61f6565f90.

<b>Name</b>	<b>Description</b>
Strike LockBit_49250b4a	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 49250b4aa060299f0c8f67349c942d1c.
Strike LockBit_5143e664	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 5143e664ed8a94496716597f7989829c.
Strike LockBit_53459a35	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 53459a35192496687d6e0137c044b342.
Strike LockBit_5761ee98	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 5761ee98b1c2fea31b5408516a8929ea.
Strike LockBit_5cc28691	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 5cc28691fdAA505b8f453e3500e3d690.
Strike LockBit_5f504bb2	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 5f504bb22471157aafEB887b4412b5de.
Strike LockBit_5f60af6d	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 5f60af6df012062182b0716343563b4f.
Strike LockBit_612a58fd	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 612a58fd67717e45d091ed3c353c3263.
Strike LockBit_6316694d	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 6316694dd1f6fd53bd04e351b86ddf70.
Strike LockBit_6744ed73	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 6744ed739ba526283864fe4917c91bb3.

<b>Name</b>	<b>Description</b>
Strike LockBit_686a20b6	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 686a20b6f55dd6aad89da2423b975c40.
Strike LockBit_75083b2b	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 75083b2b7c52eeed603559c260ad2ecf.
Strike LockBit_82b94d38	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 82b94d38457d24c62bde75f99330f762.
Strike LockBit_83958bd6	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 83958bd6ee281413f61b0d25a2bac065.
Strike LockBit_83b0fcfa1	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 83b0fcfa1bd3190c5badcea4d507b8c95.
Strike LockBit_889328e2	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 889328e2cf5f5d74531b9b0a25c1871c.
Strike LockBit_88effaad	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 88effaadb023811ae1c58235acf90c8b.
Strike LockBit_8ab03752	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 8ab0375228416b89becff72a0ae40654.
Strike LockBit_8b26b295	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 8b26b29569c5d912d1d46e0de6a84edc.
Strike LockBit_8cd0d1f9	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 8cd0d1f92240143ebe65399718a8f734.

<b>Name</b>	<b>Description</b>
Strike LockBit_9a246bf3	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 9a246bf39f3fab9c2d45f1003bdc6b45.
Strike LockBit_9dc190d6	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 9dc190d680a21eb8caeeecbd0f72d983.
Strike LockBit_9eafa10f	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 9eafa10f4014b6bbb05b5b6046f5bc67.
Strike LockBit_9fe9f4ee	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is 9fe9f4ee717bae3a5c9fdf1d380e015d.
Strike LockBit_a04a99d9	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is a04a99d946fb08b2f65ba664ad7faebd.
Strike LockBit_c0cacc5b	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is c0cacc5bf97b854b6025fe0973dc076f.
Strike LockBit_c270ab0d	This strike sends a polymorphic malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this LockBit sample is c270ab0d2922947d199777adabf851bc.
Strike LockBit_c4ee61d9	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is c4ee61d94e8b4452f7b9ad761b24905c.
Strike LockBit_cc390028	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is cc3900283ad1f0510359ead309e8debf.
Strike LockBit_e15103bb	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is e15103bb99df84bfe7f77d3bd9d54bc3.

<b>Name</b>	<b>Description</b>
Strike LockBit_e2bd98d5	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is e2bd98d575ec25a4c4b28f77776420fc.
Strike LockBit_e3a5630d	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is e3a5630d8f1a44adacc0417a064b556d.
Strike LockBit_e4179bca	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is e4179bca5bf5b1fd51172d629f5521f8.
Strike LockBit_ec273b58	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is ec273b5841eadfc43b1908c9905e95a3.
Strike LockBit_ef1cbffa	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is ef1cbffaf03936c47635549550c02567.
Strike LockBit_f3944a4e	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is f3944a4e123d56379b6cb4184de4f2ca.
Strike LockBit_f3e1802d	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is f3e1802d8ab91e9bd2e807d3af3c6d75.
Strike LockBit_f8ccb9bd	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is f8ccb9bd326744ed9d1ecc12b51b691a.
Strike LockBit_fc5e3917	This strike sends a malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The MD5 hash of this LockBit sample is fc5e3917291c1add83dc98dfe7eabee0.
Strike LockBit_fd902870	This strike sends a polymorphic malware sample known as LockBit. LockBit is a ransomware that once executed will encrypt the system files until a ransom payment has been made to the attacker. LockBit can scan and spread itself to all targets it finds on a network. The binary has the checksum removed in the PE file format. The MD5 hash of this LockBit sample is fd902870de737723e6da1e0ba10f1385.

<b>Name</b>	<b>Description</b>
Strike Locky_0158743f	This strike sends a polymorphic malware sample known as Locky. Locky is a ransomware for Windows systems which appeared at the beginning of 2016. The malicious code for this particular malware relies on JavaScript attachments to download itself. Like other ransomware, it encrypts local files as well as network shares and renames them to [unique_id][identifier].locky. The victim is requested to pay a ransom to get the files decrypted. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Locky sample is 0158743f2c7571a83669159121daed44.
Strike Locky_28b5e374	This strike sends a polymorphic malware sample known as Locky. Locky is a ransomware for Windows systems which appeared at the beginning of 2016. The malicious code for this particular malware relies on JavaScript attachments to download itself. Like other ransomware, it encrypts local files as well as network shares and renames them to [unique_id][identifier].locky. The victim is requested to pay a ransom to get the files decrypted. The binary has been packed using upx packer, with the default options. The MD5 hash of this Locky sample is 28b5e37490d59e2d5dff1c1a429263bf.
Strike Locky_37321e84	This strike sends a malware sample known as Locky. Locky is a ransomware for Windows systems which appeared at the beginning of 2016. The malicious code for this particular malware relies on JavaScript attachments to download itself. Like other ransomware, it encrypts local files as well as network shares and renames them to [unique_id][identifier].locky. The victim is requested to pay a ransom to get the files decrypted. The MD5 hash of this Locky sample is 37321e84039a822ec547de8a9aad48a9.
Strike Locky_8048aa32	This strike sends a malware sample known as Locky. Locky is a ransomware for Windows systems which appeared at the beginning of 2016. The malicious code for this particular malware relies on JavaScript attachments to download itself. Like other ransomware, it encrypts local files as well as network shares and renames them to [unique_id][identifier].locky. The victim is requested to pay a ransom to get the files decrypted. The MD5 hash of this Locky sample is 8048aa3289909b0f544bf7819a150a48.
Strike Locky_8ea1078a	This strike sends a polymorphic malware sample known as Locky. Locky is a ransomware for Windows systems which appeared at the beginning of 2016. The malicious code for this particular malware relies on JavaScript attachments to download itself. Like other ransomware, it encrypts local files as well as network shares and renames them to [unique_id][identifier].locky. The victim is requested to pay a ransom to get the files decrypted. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Locky sample is 8ea1078ae6f7500c9c1f245d69a8ce30.
Strike Locky_b73d624c	This strike sends a malware sample known as Locky. Locky is a ransomware for Windows systems which appeared at the beginning of 2016. The malicious code for this particular malware relies on JavaScript attachments to download itself. Like other ransomware, it encrypts local files as well as network shares and renames them to [unique_id][identifier].locky. The victim is requested to pay a ransom to get the files decrypted. The MD5 hash of this Locky sample is b73d624c91955ec6780053f5c6c1e552.

<b>Name</b>	<b>Description</b>
Strike Locky_cb93d5c8	This strike sends a polymorphic malware sample known as Locky. Locky is a ransomware for Windows systems which appeared at the beginning of 2016. The malicious code for this particular malware relies on JavaScript attachments to download itself. Like other ransomware, it encrypts local files as well as network shares and renames them to [unique_id][identifier].locky. The victim is requested to pay a ransom to get the files decrypted. The binary file has one more imports added in the import table. The MD5 hash of this Locky sample is cb93d5c8daa92eb0280f3ff3535b8d93.
Strike Locky_f4b19b8a	This strike sends a polymorphic malware sample known as Locky. Locky is a ransomware for Windows systems which appeared at the beginning of 2016. The malicious code for this particular malware relies on JavaScript attachments to download itself. Like other ransomware, it encrypts local files as well as network shares and renames them to [unique_id][identifier].locky. The victim is requested to pay a ransom to get the files decrypted. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Locky sample is f4b19b8a9fa2c1a3ac71e0d95acce031.
Strike Locky_fd28fdf1	This strike sends a polymorphic malware sample known as Locky. Locky is a ransomware for Windows systems which appeared at the beginning of 2016. The malicious code for this particular malware relies on JavaScript attachments to download itself. Like other ransomware, it encrypts local files as well as network shares and renames them to [unique_id][identifier].locky. The victim is requested to pay a ransom to get the files decrypted. The binary has random bytes appended at the end of the file. The MD5 hash of this Locky sample is fd28fdf16988f3400f266cc945b7fa79.
Strike LodaRAT_03f37674	This strike sends a malware sample known as LodaRAT. LodaRAT malware is a remote access tool that is written in AutoIT. It has the ability to gather information, exfiltrate data, deliver additional malware and capture screen data. This version steals cookies and passwords from Microsoft Edge and Brave. The MD5 hash of this LodaRAT sample is 03f376743e551dacf7b9eddd8d96acea.
Strike LodaRAT_24bcd132	This strike sends a malware sample known as LodaRAT. LodaRAT malware is a remote access tool that is written in AutoIT. It has the ability to gather information, exfiltrate data, deliver additional malware and capture screen data. This version steals cookies and passwords from Microsoft Edge and Brave. The MD5 hash of this LodaRAT sample is 24bcd1321b581ea0d7a00b9655a0cab2.
Strike LodaRAT_77cce071	This strike sends a malware sample known as LodaRAT. LodaRAT malware is a remote access tool that is written in AutoIT. It has the ability to gather information, exfiltrate data, deliver additional malware and capture screen data. This version steals cookies and passwords from Microsoft Edge and Brave. The MD5 hash of this LodaRAT sample is 77cce071ed220fc2e85207850909d2df.
Strike LodaRAT_81e166e0	This strike sends a malware sample known as LodaRAT. LodaRAT malware is a remote access tool that is written in AutoIT. It has the ability to gather information, exfiltrate data, deliver additional malware and capture screen data. This version steals cookies and passwords from Microsoft Edge and Brave. The MD5 hash of this LodaRAT sample is 81e166e0fe24ae2bc6c1332c3a3a7637.

<b>Name</b>	<b>Description</b>
Strike LodaRAT_8678d96c	This strike sends a malware sample known as LodaRAT. LodaRAT malware is a remote access tool that is written in AutoIT. It has the ability to gather information, exfiltrate data, deliver additional malware and capture screen data. This version steals cookies and passwords from Microsoft Edge and Brave. The MD5 hash of this LodaRAT sample is 8678d96c170a982e363b1ccb4fada460.
Strike LodaRAT_9b240a9c	This strike sends a malware sample known as LodaRAT. LodaRAT malware is a remote access tool that is written in AutoIT. It has the ability to gather information, exfiltrate data, deliver additional malware and capture screen data. This version steals cookies and passwords from Microsoft Edge and Brave. The MD5 hash of this LodaRAT sample is 9b240a9cfad431137cf86ed64bb4bdd0.
Strike LodaRAT_c2814562	This strike sends a malware sample known as LodaRAT. LodaRAT malware is a remote access tool that is written in AutoIT. It has the ability to gather information, exfiltrate data, deliver additional malware and capture screen data. This version steals cookies and passwords from Microsoft Edge and Brave. The MD5 hash of this LodaRAT sample is c281456208e2df0324fbf202e2f2c7b0.
Strike LokiBot_0160f5c8	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this LokiBot sample is 0160f5c8e9e1e2676d8d1f253ce8f8a8.
Strike LokiBot_01f2e3a9	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this LokiBot sample is 01f2e3a946d22c470784c71b442a2901.
Strike LokiBot_044a9395	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 044a9395038b80df64f21b475f2371f4.
Strike LokiBot_046776d8	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 046776d819a6a7d85b5d32fdb819cdeb.

<b>Name</b>	<b>Description</b>
Strike LokiBot_08ed7ada	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 08ed7ada50256212d5ff62819036ec92.
Strike LokiBot_0a698e88	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 0a698e8808618abeb1fbe9930d6d9fbc.
Strike LokiBot_0f454af3	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 0f454af34a3a6e3a26db1bc14e0c1ee3.
Strike LokiBot_0f58976f	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 0f58976f87aea65297d838dd4cf2ecaf.
Strike LokiBot_0f61a60e	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 0f61a60ed23ae6ca13456293649e9125.
Strike LokiBot_11f9218f	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 11f9218fbba0aa63ed8d2adcaabae67b.
Strike LokiBot_123f0bb7	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 123f0bb70e58dae81a3398cbe049c132.
Strike LokiBot_141c2a99	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 141c2a99ec6c365eefbcfe39e8dd84be3.

<b>Name</b>	<b>Description</b>
Strike LokiBot_14adebed	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this LokiBot sample is 14adebeddeb0619d03cd9509a64988c5.
Strike LokiBot_1679bcd8	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 1679bcd86e53758a0e9a8e66783002cd.
Strike LokiBot_16b925b3	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 16b925b3b891d0ba91552419b6c9a343.
Strike LokiBot_186e231b	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 186e231b1e4d0ff6626403f2c1f58906.
Strike LokiBot_1a3e6d36	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 1a3e6d3672c71fd1775411275e9322b7.
Strike LokiBot_1cbbf2c0	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 1cbbf2c0b99d2070b4e6b6e9ec77df40.
Strike LokiBot_1d2700b8	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 1d2700b86c91366053aa4e57c2b667f7.

<b>Name</b>	<b>Description</b>
Strike LokiBot_1ec5e658	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 1ec5e6588478d9336f48b25419a9c438.
Strike LokiBot_1f034f18	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 1f034f183595c871de3a55b22bed0720.
Strike LokiBot_1f5c9cb5	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 1f5c9cb59a3821f4343188b99f7437c2.
Strike LokiBot_2413fd68	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 2413fd68fc07f0ace1d515d1ae4d3995.
Strike LokiBot_24b1096d	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 24b1096dc92c31d5a7e6328520e108e7.
Strike LokiBot_29521a6c	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 29521a6c01a05faf598b406432ef1c47.
Strike LokiBot_29568752	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 29568752bc62348cadc92145fc974b78.
Strike LokiBot_298271a7	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 298271a724316ae773dfbebea4703038.

<b>Name</b>	<b>Description</b>
Strike LokiBot_2986dd0d	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 2986dd0d1fc472a96a02c5ef9644c1d8.
Strike LokiBot_2992b0b0	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 2992b0b080ab66fcd660f9e1f6db0e6d.
Strike LokiBot_2ae52ed0	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 2ae52ed06d8466acf2ba526c9808c44c.
Strike LokiBot_2c4b9f71	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 2c4b9f716576fd4687556af2aa882e1f.
Strike LokiBot_2cd7b4b2	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 2cd7b4b2357cc3a9f632f2c6efd120ec.
Strike LokiBot_2f6f3af9	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary file has one more imports added in the import table. The MD5 hash of this LokiBot sample is 2f6f3af90b6df93d8d98909ca888a2ed.
Strike LokiBot_307fee76	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 307fee76a6790b07f15db9f78204d0a7.

<b>Name</b>	<b>Description</b>
Strike LokiBot_311d9241	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 311d92417b9093f29f297805272725c3.
Strike LokiBot_32270e69	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 32270e6929682c0ae0fdb255ff1ed6d5.
Strike LokiBot_3270fa89	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 3270fa8988eb62bdb1c08a04543a6fb9.
Strike LokiBot_33102be1	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 33102be1cea0e73e32be5ccf17c4764d.
Strike LokiBot_35208fcf	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 35208fcf5f72ad26feffc3c77f0b53d9.
Strike LokiBot_353c4d62	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 353c4d6259b7f63eb1a723d2ee125bb1.
Strike LokiBot_373972b4	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 373972b442618f90e904e77366758271.
Strike LokiBot_393264b4	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 393264b41d8cb7b93d7cc3e079556eff.

<b>Name</b>	<b>Description</b>
Strike LokiBot_3d61b1e8	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 3d61b1e8349089f3db639532f9afcc70.
Strike LokiBot_3d699bcf	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 3d699bcfc5b1f7f20ed2668c45e8ddcc.
Strike LokiBot_3ed3394c	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 3ed3394cd0761470aabdd911634c59d6.
Strike LokiBot_3f2e9256	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 3f2e92568e3e77e88dc3a0ffb6755a79.
Strike LokiBot_41aa2de6	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 41aa2de67067959254211d5970c35c63.
Strike LokiBot_42a27b7b	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 42a27b7b122f8e048980c0e7bf04b5c9.
Strike LokiBot_4389ba6f	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this LokiBot sample is 4389ba6f50000c82a7118a2d1015eadf.

<b>Name</b>	<b>Description</b>
Strike LokiBot_43b38e77	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 43b38e775099053f93f72ac9ab5bfc25.
Strike LokiBot_44fc10c3	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 44fc10c3b6cc2f42d2dacd19f9219915.
Strike LokiBot_45189936	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 45189936f6062b0e81a7dc44e3c1c6e7.
Strike LokiBot_47026faf	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 47026fafcb973ba3387e8c97f6871bb1.
Strike LokiBot_495fff18	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 495fff18bc8c631e44c00b273d0742d2.
Strike LokiBot_4973f991	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 4973f991a4f80bb49052af30e8922a17.
Strike LokiBot_4b043d0f	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 4b043d0fccca4bea612f21dd3a4d7fd9.
Strike LokiBot_4d198d9c	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 4d198d9c0564a594ce46be7bce19edd6.

<b>Name</b>	<b>Description</b>
Strike LokiBot_4e52a06f	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 4e52a06feec62c667f65ab9ffa4e1867.
Strike LokiBot_4edfba05	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random bytes appended at the end of the file. The MD5 hash of this LokiBot sample is 4edfba05c275b53b5a4e569ea760160c.
Strike LokiBot_502187ce	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 502187ce6d5d1f537c244b90435e9ca9.
Strike LokiBot_53b771d0	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 53b771d049bacdd030fe2424b9f7a7ef.
Strike LokiBot_572ee199	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 572ee199d9d6793f1b6f5a8696bb6532.
Strike LokiBot_574ea378	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 574ea37878e74bbcf646402baf723ee4.
Strike LokiBot_5885b5c9	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 5885b5c94d4e34a250d8e325a0727578.

<b>Name</b>	<b>Description</b>
Strike LokiBot_589813a9	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 589813a949474184438f1b7117457913.
Strike LokiBot_59b388de	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 59b388dee247bcecd66795063b0c02d7.
Strike LokiBot_5c5ad7f3	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 5c5ad7f35533f46e30133dba9186d4b1.
Strike LokiBot_5cc22a11	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this LokiBot sample is 5cc22a110c449112b320edf81f3b3330.
Strike LokiBot_5d6e02f7	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random bytes appended at the end of the file. The MD5 hash of this LokiBot sample is 5d6e02f77ca51f9a8d22da843ee87791.
Strike LokiBot_5dde0410	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 5dde041006ed3df18d4820a8b5208c09.
Strike LokiBot_5e0f32cb	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 5e0f32cb907fa23b7d4dc8c684e9720b.

<b>Name</b>	<b>Description</b>
Strike LokiBot_630f9c03	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 630f9c038b9d219998a29dda39680060.
Strike LokiBot_634d500f	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 634d500f4ee3781a34e23394e57126dd.
Strike LokiBot_63e3bfaa	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 63e3bfaaa31cc2014010270ecfbc72be.
Strike LokiBot_64af1511	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 64af151191f5d60b7ace7a8cb31e7948.
Strike LokiBot_67f5daf1	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has the checksum removed in the PE file format. The MD5 hash of this LokiBot sample is 67f5daf17df5a86d4a89d9318402b84d.
Strike LokiBot_6882fe2e	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 6882fe2e90093a2bfd5d96371330e809.
Strike LokiBot_68c7222e	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 68c7222eb38c3fe88087cca91120bbe0.

<b>Name</b>	<b>Description</b>
Strike LokiBot_6bffac8e	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 6bffac8eeb297dd82fecf271f408ee81.
Strike LokiBot_6c2cd24b	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 6c2cd24b96a7cf4f1a2d4e4ba2b05453.
Strike LokiBot_6c8a1688	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 6c8a16888e371f15f0b018fb0ddaae2e.
Strike LokiBot_6f06a830	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 6f06a830e7610d4f2e9a1a5c2a4b542b.
Strike LokiBot_6f0a7ddc	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 6f0a7ddcbcf4446f2d2d230bff72a356.
Strike LokiBot_754ba410	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 754ba4100095de1dfb830d226af267eb.
Strike LokiBot_757d1361	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 757d13617a9b81777d56e85544fc1855.
Strike LokiBot_75aa607a	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 75aa607a9f8bf2af141de19a41b0bd94.

<b>Name</b>	<b>Description</b>
Strike LokiBot_760b6e1b	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 760b6e1b06322fbe556f9ddf683b0389.
Strike LokiBot_77393a98	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 77393a984431fb546e97beb9d0e060b3.
Strike LokiBot_78a38cf3	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 78a38cf302c4722b6c3ac5c66e227ca1.
Strike LokiBot_7a2ae5d5	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 7a2ae5d579597b4d8a6806011501e92a.
Strike LokiBot_7ac770ca	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 7ac770caa432948e3fccfe11d2e3b723.
Strike LokiBot_7c00e0bf	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 7c00e0bf99464c5067a4d8440d605c90.
Strike LokiBot_7cb30279	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 7cb30279f0488c9418ae1a2d080699b9.

<b>Name</b>	<b>Description</b>
Strike LokiBot_7eecfc0d	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this LokiBot sample is 7eecfc0d8fff84b306e0bbade7c6c6a3.
Strike LokiBot_81ea5d32	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 81ea5d3263580f61029ac0c028f70e62.
Strike LokiBot_83c8c724	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 83c8c724740f88b6f565cf5698764a3f.
Strike LokiBot_84f21713	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 84f21713a93c0c1da2be63ca7ee14815.
Strike LokiBot_862e155b	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this LokiBot sample is 862e155bf0110e49edb1f26847b9d4c0.
Strike LokiBot_884f39ae	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 884f39ae4c80b09eaa37deaeb9b2d42c.
Strike LokiBot_88f32078	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 88f320782e23977a4877c517646c3ff8.

<b>Name</b>	<b>Description</b>
Strike LokiBot_89e9dbf2	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this LokiBot sample is 89e9dbf2546d9f1949c3ae8b7e16ce12.
Strike LokiBot_8caa05af	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 8caa05af7060f02bab07ccfba6ac42d6.
Strike LokiBot_8cf06eab	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 8cf06eabe64b0230580550be88d4d5f5.
Strike LokiBot_8fad80b1	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 8fad80b104bd3234323be9171aed903f.
Strike LokiBot_9080d22e	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has been packed using upx packer, with the default options. The MD5 hash of this LokiBot sample is 9080d22e80227fff2e55c42ca53b4061.
Strike LokiBot_90d6eeb7	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 90d6eeb774dfc96b215d0ebea5464640.
Strike LokiBot_91b4e621	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 91b4e6212de5a3db83fee9d1c0c9ca56.

<b>Name</b>	<b>Description</b>
Strike LokiBot_91f28ad2	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 91f28ad2f9c1abf319254e802ff35ecf.
Strike LokiBot_928bd458	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 928bd4584eac8e3b8393510bb010cd20.
Strike LokiBot_92ccd05c	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 92ccd05c0b161385f503bd62c2f87995.
Strike LokiBot_92d1f7e5	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 92d1f7e5f1d35e4c3744798b583da7e8.
Strike LokiBot_933cb353	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 933cb35362f832513bd168c62ef1eb1f.
Strike LokiBot_944824b4	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this LokiBot sample is 944824b422c4603b89cc48a8a68420f6.
Strike LokiBot_95105b9f	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 95105b9f79ad64a5187f3859a6e74347.

<b>Name</b>	<b>Description</b>
Strike LokiBot_97351713	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random bytes appended at the end of the file. The MD5 hash of this LokiBot sample is 97351713c1c618911aedc95981242a15.
Strike LokiBot_985dcd1f	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random bytes appended at the end of the file. The MD5 hash of this LokiBot sample is 985dcd1f24eba6bb96148752cc35bd28.
Strike LokiBot_9a1f1689	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 9a1f1689b94d59c040af83f496ba5bbb.
Strike LokiBot_9a4c1fb2	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random bytes appended at the end of the file. The MD5 hash of this LokiBot sample is 9a4c1fb2d9f082a73e5bddc76573d1b3.
Strike LokiBot_9a53b56a	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 9a53b56adece33768f427031a3e068d.
Strike LokiBot_9c3d5fda	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 9c3d5fda30d4b32841708d7d7f99c62a.
Strike LokiBot_9cfa5f2f	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 9cfa5f2f4aacce5f0f676f2e3b32663f.

<b>Name</b>	<b>Description</b>
Strike LokiBot_9d420f07	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 9d420f07ba12c973e525b788c36341a3.
Strike LokiBot_9e4f03f3	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 9e4f03f3d598a06898632f10b4eaec6a.
Strike LokiBot_9ec2a2e6	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is 9ec2a2e68f07d83c5904dde328c2f594.
Strike LokiBot_a0294d29	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this LokiBot sample is a0294d29cced97c582a53fd7e42922ee.
Strike LokiBot_a4e9151e	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is a4e9151e7fcc3e22e4be8030681c6781.
Strike LokiBot_a85424f2	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is a85424f2fb6f690b5f336928355673d1.
Strike LokiBot_a862611c	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is a862611c1be0659cbde96a3d3f79ba61.

<b>Name</b>	<b>Description</b>
Strike LokiBot_aa697c8d	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is aa697c8d518ad8c3a01d9146db11335b.
Strike LokiBot_ab04f52f	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has the checksum removed in the PE file format. The MD5 hash of this LokiBot sample is ab04f52f3035256aa8b91ad784fd6724.
Strike LokiBot_ad2af567	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has been packed using upx packer, with the default options. The MD5 hash of this LokiBot sample is ad2af56777bc68b392ff58168defd2db.
Strike LokiBot_ad3e77ee	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is ad3e77ee78c0fa6b352b8c5ba99d3255.
Strike LokiBot_ad5b37cf	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is ad5b37cf2635524fb9111057c593b57.
Strike LokiBot_b16e4e70	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is b16e4e70f692bc53b71d54679e63af6e.
Strike LokiBot_b18fa4c6	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this LokiBot sample is b18fa4c6266d7f4e46f4f8151d255273.

<b>Name</b>	<b>Description</b>
Strike LokiBot_b18fd4de	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is b18fd4de724718b8d1fa887d94731da4.
Strike LokiBot_b1e0d2ea	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is b1e0d2ead352745d57ea43c58f18aadf.
Strike LokiBot_b4db3566	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is b4db3566b4b1e540025a20a3e826ad71.
Strike LokiBot_b6b1d041	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this LokiBot sample is b6b1d0412d31a02bfa8c1a6a85ef8ffa.
Strike LokiBot_b7469cbe	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this LokiBot sample is b7469cbefbbfec180dff5419489b8e5a.
Strike LokiBot_b75a41ad	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is b75a41ad2dcabea1deec1e893ee3f3bc.
Strike LokiBot_b9697256	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is b969725644870466de0f63d8d67d5b1d.

<b>Name</b>	<b>Description</b>
Strike LokiBot_bb112ab2	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is bb112ab2ef7c240940753d7bb9dcf8e9.
Strike LokiBot_bce8d497	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is bce8d497ea21fe3fee999190ed628c98.
Strike LokiBot_bd8d5c28	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is bd8d5c28da2adb86149bf00a3ea71ca9.
Strike LokiBot_c102ca2e	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is c102ca2e4e64d11889524a1b56fc4ad.
Strike LokiBot_c1579bc6	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is c1579bc69d2861973aae40e76fe10626.
Strike LokiBot_c198fc14	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is c198fc143d8160a8f3de9ee1725c5193.
Strike LokiBot_c1cb29e7	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is c1cb29e7ba19799e20fae14ffa698418.
Strike LokiBot_c2d963dd	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is c2d963dd959c1634e35bc1ccc1292174.

<b>Name</b>	<b>Description</b>
Strike LokiBot_c5c06432	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is c5c06432bc7c0780e0de5028dd4098c4.
Strike LokiBot_c6582fc0	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is c6582fc0d09ccf4f8bb82b06b5c40935.
Strike LokiBot_c8a47262	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is c8a472629bb9193b37b9156b91672bc9.
Strike LokiBot_ce3ac223	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is ce3ac2236b1cdd0a2695dce6ba384477.
Strike LokiBot_ceb9237e	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is ceb9237ecded700afae826f03d43c80c.
Strike LokiBot_cf156148	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is cf1561485f3bae2ae2e9ba8a09a28e3d.
Strike LokiBot_cf7dadad	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is cf7dadad5ee54a4a2cf74f8cf5f4ffbb.
Strike LokiBot_d2cf28ad	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is d2cf28ad06a13f24e906790eae874fb3.

<b>Name</b>	<b>Description</b>
Strike LokiBot_d59102dc	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is d59102dcc956a859de8d5c6545b30bfd.
Strike LokiBot_d837beeb	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this LokiBot sample is d837beeb7c4e69aba79da8831e22cccd8.
Strike LokiBot_dcf9cbe7	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is dcf9cbe7ae9f37c58edc4f37821a44da.
Strike LokiBot_ddd0e23f	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is ddd0e23fed0e19f7cd079acc1d6e546c.
Strike LokiBot_de433e93	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is de433e93de690982cfb81edf103f084b.
Strike LokiBot_deee41bf	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is deeee41bfad6e302d1a7ceebb22f66abb.
Strike LokiBot_df3e2f50	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has been packed using upx packer, with the default options. The MD5 hash of this LokiBot sample is df3e2f50ba42ae245bf30f052fb5ec48.

<b>Name</b>	<b>Description</b>
Strike LokiBot_e0475490	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random bytes appended at the end of the file. The MD5 hash of this LokiBot sample is e0475490016be0843632565d4f980d11.
Strike LokiBot_e2d55f15	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is e2d55f15beeecc19914b40971a0f413e.
Strike LokiBot_e2f72215	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this LokiBot sample is e2f7221545da3787b1ad45c0e245f0e1.
Strike LokiBot_e378a018	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is e378a01869a371d579f14129b6ef6c7b.
Strike LokiBot_e91bf0df	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is e91bf0df1a84194f47797703938a180b.
Strike LokiBot_e9e7330e	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is e9e7330eb919f75746cbd2018d1b06f4.
Strike LokiBot_eb6e6f02	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is eb6e6f029fb992c914f3ef7ec14ac26d.

<b>Name</b>	<b>Description</b>
Strike LokiBot_eb9603a9	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is eb9603a9904e78f85911398887281718.
Strike LokiBot_eca2cb25	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is eca2cb25c919294dcaec338b4ba882d5.
Strike LokiBot_f176e605	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is f176e6052a3f5832a24ab1d55eda274e.
Strike LokiBot_f22fa361	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is f22fa36134c5405dad05e172bdef8edf.
Strike LokiBot_f3821f00	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is f3821f00986bcfae38622179fc49f5c.
Strike LokiBot_f520c950	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is f520c950b540931fb502ad1fcc6e5ec.
Strike LokiBot_f696499b	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is f696499b3888e3cedefce687917c127d.
Strike LokiBot_f977b8f3	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is f977b8f3919dc992d6ffe3fd0505815a.

<b>Name</b>	<b>Description</b>
Strike LokiBot_fd81a8e6	This strike sends a polymorphic malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The binary has random bytes appended at the end of the file. The MD5 hash of this LokiBot sample is fd81a8e64de9f065551f77558849e86e.
Strike LokiBot_feb2366b	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is feb2366b62e5204c8b4f70efc8a297d0.
Strike LokiBot_fecc5f1d	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is fecc5f1d5740f7ed686283629c08f854.
Strike LokiBot_ff0e4f8a	This strike sends a malware sample known as LokiBot. Lokibot is an information-stealing malware designed to siphon off sensitive information stored on an infected device. It is modular in nature, supporting the ability to steal sensitive information from a number of popular applications. It is commonly pushed via malicious documents delivered via spam emails. The MD5 hash of this LokiBot sample is ff0e4f8a8a1bdd195568c08aa7ed885b.
Strike Lumma Stealer_04487597	This strike sends a malware sample known as Lumma Stealer. Lumma Stealer is an information stealer malware. Primarily it has been used to target cryptocurrency wallets and browser extensions. Most recently it has been associated with the cloud-based data storage company, Snowflake's data breach. Once information is obtained it is exfiltrated typically through HTTP POST requests back to the attacker. The MD5 hash of this Lumma Stealer sample is 044875973275dfdce9b96bfe37926ad3.
Strike Lumma Stealer_0d83ff89	This strike sends a malware sample known as Lumma Stealer. Lumma Stealer is an information stealer malware. Primarily it has been used to target cryptocurrency wallets and browser extensions. Most recently it has been associated with the cloud-based data storage company, Snowflake's data breach. Once information is obtained it is exfiltrated typically through HTTP POST requests back to the attacker. The MD5 hash of this Lumma Stealer sample is 0d83ff899ff8fcfdb8ebe805401a9c19.
Strike Lumma Stealer_1906650c	This strike sends a malware sample known as Lumma Stealer. Lumma Stealer is an information stealer malware. Primarily it has been used to target cryptocurrency wallets and browser extensions. Most recently it has been associated with the cloud-based data storage company, Snowflake's data breach. Once information is obtained it is exfiltrated typically through HTTP POST requests back to the attacker. The MD5 hash of this Lumma Stealer sample is 1906650c3f390bab2e00a9d27b60a230.

<b>Name</b>	<b>Description</b>
Strike Lumma Stealer_30aa7255	This strike sends a malware sample known as Lumma Stealer. Lumma Stealer is an information stealer malware. Primarily it has been used to target cryptocurrency wallets and browser extensions. Most recently it has been associated with the cloud-based data storage company, Snowflake's data breach. Once information is obtained it is exfiltrated typically through HTTP POST requests back to the attacker. The MD5 hash of this Lumma Stealer sample is 30aa7255a82ad8b9edf092f79adcd87d.
Strike Lumma Stealer_3e3f9ee5	This strike sends a malware sample known as Lumma Stealer. Lumma Stealer is an information stealer malware. Primarily it has been used to target cryptocurrency wallets and browser extensions. Most recently it has been associated with the cloud-based data storage company, Snowflake's data breach. Once information is obtained it is exfiltrated typically through HTTP POST requests back to the attacker. The MD5 hash of this Lumma Stealer sample is 3e3f9ee5b7dfa6b779664059dd7ab9f.
Strike Lumma Stealer_c9c0e32e	This strike sends a malware sample known as Lumma Stealer. Lumma Stealer is an information stealer malware. Primarily it has been used to target cryptocurrency wallets and browser extensions. Most recently it has been associated with the cloud-based data storage company, Snowflake's data breach. Once information is obtained it is exfiltrated typically through HTTP POST requests back to the attacker. The MD5 hash of this Lumma Stealer sample is c9c0e32e00d084653db0b37a239e9a34.
Strike Lumma Stealer_ef3a8da8	This strike sends a malware sample known as Lumma Stealer. Lumma Stealer is an information stealer malware. Primarily it has been used to target cryptocurrency wallets and browser extensions. Most recently it has been associated with the cloud-based data storage company, Snowflake's data breach. Once information is obtained it is exfiltrated typically through HTTP POST requests back to the attacker. The MD5 hash of this Lumma Stealer sample is ef3a8da845a07305fb5f38f3221e8290.
Strike Lumma Stealer_fc566dde	This strike sends a malware sample known as Lumma Stealer. Lumma Stealer is an information stealer malware. Primarily it has been used to target cryptocurrency wallets and browser extensions. Most recently it has been associated with the cloud-based data storage company, Snowflake's data breach. Once information is obtained it is exfiltrated typically through HTTP POST requests back to the attacker. The MD5 hash of this Lumma Stealer sample is fc566dde5de9d2b7a66e2132c8acbc80.
Strike LunarSpider_21cde10c	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 21cde10c7da48bab622e75d6004d61de.

<b>Name</b>	<b>Description</b>
Strike LunarSpider_2a743bcc	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 2a743bcc9cee1900a0457127abeade60.
Strike LunarSpider_2c3d09cd	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 2c3d09cd1d8aea8cc7049296782c8def.
Strike LunarSpider_330a6bae	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 330a6bae00ad4be4a0df732520905395.
Strike LunarSpider_33f6c6b3	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 33f6c6b3727a233819111e3b3aae96ec.
Strike LunarSpider_3f21939c	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 3f21939c7db0c894b74c361d72d044db.

<b>Name</b>	<b>Description</b>
Strike LunarSpider_56d21ac3	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 56d21ac3631f52b18325224214dcbd73.
Strike LunarSpider_628d88e9	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 628d88e98c44d9846954fd47bbb8e143.
Strike LunarSpider_66b559df	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 66b559df3b20b0280322e9bf67752d6a.
Strike LunarSpider_97be7a2e	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is 97be7a2e8918be589396de0eaf97a590.
Strike LunarSpider_a0ffaf70	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is a0ffaf708b8c44e7fd3a5a505acc015b.

<b>Name</b>	<b>Description</b>
Strike LunarSpider_a3254b2e	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is a3254b2ef6bca343aa158261d7a46c50.
Strike LunarSpider_d58be0d4	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is d58be0d4dcc144ca9d6a1ecf9e8232f9.
Strike LunarSpider_e0df61c7	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is e0df61c7e5c764396970dd47d4589c01.
Strike LunarSpider_fd817202	This strike sends a malware sample known as LunarSpider. Lunar Spider is a malware of the banking trojan family that is used to steal financial information and facilitate further compromise. It is delivered primarily via malvertising and email campaigns, which lead victims to a fake CAPTCHA webpage that tricks them into downloading a malicious installer. When executed, the installer loads the IcedID payload and establishes persistence on the infected system. Its key capabilities include credential theft, collection of banking information, system reconnaissance, and enabling follow-on access for additional malware deployment. The MD5 hash of this LunarSpider sample is fd817202314d4067c2dc9c51d98f0268.
Strike Lydra_06fa2eb4	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is 06fa2eb46ad814569baadb2549fd27c3.
Strike Lydra_0af3b3f7	This strike sends a polymorphic malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Lydra sample is 0af3b3f763055e7c0437e5f0b57eaeaf.

<b>Name</b>	<b>Description</b>
Strike Lydرا_0eddb35f	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is 0eddb35f4053a1560d8e615a692bacf2.
Strike Lydرا_1197632f	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is 1197632f08b212c0eaa0826a24126771.
Strike Lydرا_1770b93c	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is 1770b93c9a0507f45d89744818055350.
Strike Lydرا_26d60427	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is 26d6042786097f5611ca308e85cf45fa.
Strike Lydرا_2afe516c	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is 2afe516c0fc84c348396394f2222d3df.
Strike Lydرا_2cf374f0	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is 2cf374f0fc3fe25804ccf3a30d30362d.
Strike Lydرا_3b96101a	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is 3b96101a3bb9fc85a0dc6992a465384.
Strike Lydرا_5997ac16	This strike sends a polymorphic malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Lydra sample is 5997ac16c6a669d83b99a296289c71b8.
Strike Lydرا_5eb3637d	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is 5eb3637da49f89486eb76a70cdbd4ed7.
Strike Lydرا_5f1583c9	This strike sends a polymorphic malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The binary has random bytes appended at the end of the file. The MD5 hash of this Lydra sample is 5f1583c98600b138a80b5940dc48b78d.
Strike Lydرا_6a56292d	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is 6a56292dca5d844048c166288dfb8d12.

<b>Name</b>	<b>Description</b>
Strike Lydرا_74059b01	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is 74059b0184b8ca790207caa5ef25680c.
Strike Lydرا_77eb6d25	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is 77eb6d2555b1bf5020c3ed6c96c36914.
Strike Lydرا_801ec30d	This strike sends a polymorphic malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The binary has random bytes appended at the end of the file. The MD5 hash of this Lydra sample is 801ec30dfa8188cc0c6a81955564956e.
Strike Lydرا_840710a5	This strike sends a polymorphic malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Lydra sample is 840710a56264b708f3eb3bbbc5c1321d.
Strike Lydرا_a6bbb58c	This strike sends a polymorphic malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Lydra sample is a6bbb58c1f7c4f0922dfd96c4b79236f.
Strike Lydرا_afec8070	This strike sends a polymorphic malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Lydra sample is afec8070f50efcc17d2ed37ecbb62836.
Strike Lydرا_be8460bd	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is be8460bd64827960aea8b219e2d3fb3a.
Strike Lydرا_c38cc376	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is c38cc3765d0716273c8ed79329236862.
Strike Lydرا_c92de4ae	This strike sends a polymorphic malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Lydra sample is c92de4ae19118495095c6c37af78ac10.
Strike Lydرا_cd9194b6	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is cd9194b61a41fa54750c3a0c8c8213b6.

<b>Name</b>	<b>Description</b>
Strike Lydرا_d432eb6e	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is d432eb6ee625acd6397249c1aa090832.
Strike Lydرا_d5c033ac	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is d5c033ac824b36409ef2db6ffc040fe6.
Strike Lydرا_d7a51c98	This strike sends a polymorphic malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Lydra sample is d7a51c9826dbb49d8231ec75fa41e0e2.
Strike Lydرا_dc303021	This strike sends a polymorphic malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Lydra sample is dc3030213c6d17ccad1dff4bc9201872.
Strike Lydرا_efceda07	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is efceda078559280ccc602f9ddc4dec45.
Strike Lydرا_fd5fe179	This strike sends a malware sample known as Lydra. Lydra is malware that steals sensitive information like passwords and setups various persist mechanisms to ensure execution at startup. The MD5 hash of this Lydra sample is fd5fe1794394752c0731c8bfad7ef61d.
Strike MQsTTang RAR_12ff186b	This strike sends a malware sample known as MQsTTang RAR. MQsTTang is malware backdoor that has been attributed to the Mustang Panda APT group. This group has focused primarily on political organizations in Europe and Asia. The Mustang Panda group uses phishing emails to distribute the malware and Github to host the payloads. Once executed the malware duplicates itself and begins enabling persistence by creating a registry key. The malware communicates to the C2 server via the MQTT protocol and includes functionality to detect debugging and monitoring tools in order to evade detection. This file is the RAR archive used to distribute MQSTTang. The MD5 hash of this MQsTTang RAR sample is 12ff186b75297382ef4fcc3f23b9a73e.
Strike MQsTTang RAR_3017fd57	This strike sends a malware sample known as MQsTTang RAR. MQsTTang is malware backdoor that has been attributed to the Mustang Panda APT group. This group has focused primarily on political organizations in Europe and Asia. The Mustang Panda group uses phishing emails to distribute the malware and Github to host the payloads. Once executed the malware duplicates itself and begins enabling persistence by creating a registry key. The malware communicates to the C2 server via the MQTT protocol and includes functionality to detect debugging and monitoring tools in order to evade detection. This file is the RAR archive used to distribute MQSTTang. The MD5 hash of this MQsTTang RAR sample is 3017fd573639f7cc0f82b941becc18ca.

Name	Description
Strike MQsTTang RAR_b26099e4	This strike sends a malware sample known as MQsTTang RAR. MQsTTang is malware backdoor that has been attributed to the Mustang Panda APT group. This group has focused primarily on political organizations in Europe and Asia. The Mustang Panda group uses phishing emails to distribute the malware and Github to host the payloads. Once executed the malware duplicates itself and begins enabling persistence by creating a registry key. The malware communicates to the C2 server via the MQTT protocol and includes functionality to detect debugging and monitoring tools in order to evade detection. This file is the RAR archive used to distribute MQSTTang. The MD5 hash of this MQsTTang RAR sample is b26099e4d1af79e5d4c8cec7888e50e4.
Strike MQsTTang_25b40859	This strike sends a malware sample known as MQsTTang. MQsTTang is malware backdoor that has been attributed to the Mustang Panda APT group. This group has focused primarily on political organizations in Europe and Asia. The Mustang Panda group uses phishing emails to distribute the malware and Github to host the payloads. Once executed the malware duplicates itself and begins enabling persistence by creating a registry key. The malware communicates to the C2 server via the MQTT protocol and includes functionality to detect debugging and monitoring tools in order to evade detection. This file is the MQSTTang backdoor. The MD5 hash of this MQsTTang sample is 25b40859cfbf2505ada54461c63f89ba.
Strike MQsTTang_85278719	This strike sends a malware sample known as MQsTTang. MQsTTang is malware backdoor that has been attributed to the Mustang Panda APT group. This group has focused primarily on political organizations in Europe and Asia. The Mustang Panda group uses phishing emails to distribute the malware and Github to host the payloads. Once executed the malware duplicates itself and begins enabling persistence by creating a registry key. The malware communicates to the C2 server via the MQTT protocol and includes functionality to detect debugging and monitoring tools in order to evade detection. This file is the MQSTTang backdoor. The MD5 hash of this MQsTTang sample is 852787190a2d4842c5812b2084982efa.
Strike MQsTTang_bff4ce3d	This strike sends a malware sample known as MQsTTang. MQsTTang is malware backdoor that has been attributed to the Mustang Panda APT group. This group has focused primarily on political organizations in Europe and Asia. The Mustang Panda group uses phishing emails to distribute the malware and Github to host the payloads. Once executed the malware duplicates itself and begins enabling persistence by creating a registry key. The malware communicates to the C2 server via the MQTT protocol and includes functionality to detect debugging and monitoring tools in order to evade detection. This file is the MQSTTang backdoor. The MD5 hash of this MQsTTang sample is bff4ce3dbda522e92970c5d1d0471e63.
Strike MQsTTang_f6e479bd	This strike sends a malware sample known as MQsTTang. MQsTTang is malware backdoor that has been attributed to the Mustang Panda APT group. This group has focused primarily on political organizations in Europe and Asia. The Mustang Panda group uses phishing emails to distribute the malware and Github to host the payloads. Once executed the malware duplicates itself and begins enabling persistence by creating a registry key. The malware communicates to the C2 server via the MQTT protocol and includes functionality to detect debugging and monitoring tools in order to evade detection. This file is the MQSTTang backdoor. The MD5 hash of this MQsTTang sample is f6e479bdc53af2f095fd9257c5cd6bcc.

<b>Name</b>	<b>Description</b>
Strike MacStealer_00700cd3	This strike sends a malware sample known as MacStealer. MacStealer is a macOS malware that uses the Telegram messaging application to conduct its C2 operations. This malware can steal documents and browser cookies as well as user logon information. The MD5 hash of this MacStealer sample is 00700cd3870716e0317479ad5e2307aa.
Strike MacStealer_0dcf52a9	This strike sends a malware sample known as MacStealer. MacStealer is a macOS malware that uses the Telegram messaging application to conduct its C2 operations. This malware can steal documents and browser cookies as well as user logon information. The MD5 hash of this MacStealer sample is 0dcf52a9567644912f24ff230f2cb39f.
Strike MacStealer_2478e0b0	This strike sends a malware sample known as MacStealer. MacStealer is a macOS malware that uses the Telegram messaging application to conduct its C2 operations. This malware can steal documents and browser cookies as well as user logon information. The MD5 hash of this MacStealer sample is 2478e0b0eb6a77f06826549244f66643.
Strike MacStealer_4b9c69fb	This strike sends a malware sample known as MacStealer. MacStealer is a macOS malware that uses the Telegram messaging application to conduct its C2 operations. This malware can steal documents and browser cookies as well as user logon information. The MD5 hash of this MacStealer sample is 4b9c69fb12988796f94b9bffeaddbb6d.
Strike MacStealer_4c23ad4a	This strike sends a malware sample known as MacStealer. MacStealer is a macOS malware that uses the Telegram messaging application to conduct its C2 operations. This malware can steal documents and browser cookies as well as user logon information. The MD5 hash of this MacStealer sample is 4c23ad4a7a4d1c4516644387bf4c9e2e.
Strike MacStealer_4ca55bbc	This strike sends a malware sample known as MacStealer. MacStealer is a macOS malware that uses the Telegram messaging application to conduct its C2 operations. This malware can steal documents and browser cookies as well as user logon information. The MD5 hash of this MacStealer sample is 4ca55bbcfdbd546e5420c8fd0f4c05c2.
Strike MacStealer_67105c73	This strike sends a malware sample known as MacStealer. MacStealer is a macOS malware that uses the Telegram messaging application to conduct its C2 operations. This malware can steal documents and browser cookies as well as user logon information. The MD5 hash of this MacStealer sample is 67105c73b8a7ee319417aff902c9c015.
Strike MacStealer_99b23ab6	This strike sends a malware sample known as MacStealer. MacStealer is a macOS malware that uses the Telegram messaging application to conduct its C2 operations. This malware can steal documents and browser cookies as well as user logon information. The MD5 hash of this MacStealer sample is 99b23ab618527277b2108e0bc06e7edd.
Strike MacStealer_9ad4172e	This strike sends a malware sample known as MacStealer. MacStealer is a macOS malware that uses the Telegram messaging application to conduct its C2 operations. This malware can steal documents and browser cookies as well as user logon information. The MD5 hash of this MacStealer sample is 9ad4172e7d69aa80844e50c1bafda2dc.

<b>Name</b>	<b>Description</b>
Strike MacStealer_c08d71b3	This strike sends a malware sample known as MacStealer. MacStealer is a macOS malware that uses the Telegram messaging application to conduct its C2 operations. This malware can steal documents and browser cookies as well as user logon information. The MD5 hash of this MacStealer sample is c08d71b3c42396f046d91955fcf3d966.
Strike MacStealer_c1ed7122	This strike sends a malware sample known as MacStealer. MacStealer is a macOS malware that uses the Telegram messaging application to conduct its C2 operations. This malware can steal documents and browser cookies as well as user logon information. The MD5 hash of this MacStealer sample is c1ed7122a1de47a0b46510eaec5346eb.
Strike MacStealer_cc5bf90f	This strike sends a malware sample known as MacStealer. MacStealer is a macOS malware that uses the Telegram messaging application to conduct its C2 operations. This malware can steal documents and browser cookies as well as user logon information. The MD5 hash of this MacStealer sample is cc5bf90f256e363fc0d4f48ecdc0706d.
Strike MacStealer_e966bf21	This strike sends a malware sample known as MacStealer. MacStealer is a macOS malware that uses the Telegram messaging application to conduct its C2 operations. This malware can steal documents and browser cookies as well as user logon information. The MD5 hash of this MacStealer sample is e966bf21c1c69b3dcebd4da19c08466.
Strike Mandrake_1b579842	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is 1b579842077e0ec75346685ffd689d6e.
Strike Mandrake_202b5c05	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is 202b5c0591e1ae09f9021e6aad5e8a8b.
Strike Mandrake_3837a060	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is 3837a06039682ced414a9a7bec7de1ef.

Name	Description
Strike Mandrake_3c2c9c6c	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is 3c2c9c6ca906ea6c6d993efd0f2dc40e.
Strike Mandrake_49468779	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is 494687795592106574edfccef27729e.
Strike Mandrake_5d77f2f5	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is 5d77f2f59aade2d1656eb7506bd02cc9.
Strike Mandrake_79f8be1e	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is 79f8be1e5c050446927d4e4facff279c.
Strike Mandrake_7f1805ec	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is 7f1805ec0187ddb54a55eabe3e2396f5.

Name	Description
Strike Mandrake_8523262a	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is 8523262a411e4d8db2079ddac8424a98.
Strike Mandrake_8dcbed73	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is 8dcbed733f5abf9bc5a574de71a3ad53.
Strike Mandrake_95d3e260	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is 95d3e26071506c6695a3760b97c91d75.
Strike Mandrake_984b3364	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is 984b336454282e7a0fb62d55edfb890a.
Strike Mandrake_a18a0457	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is a18a0457d0d4833add2dc6eac1b0b323.

Name	Description
Strike Mandrake_da110867	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is da1108674eb3f77df2fee10d116cc685.
Strike Mandrake_eb595fbc	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is eb595fbef24f94c329ac0e6ba63fe984.
Strike Mandrake_f0ae0c43	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, to evade detection and infiltrate official app marketplaces. The MD5 hash of this Mandrake sample is f0ae0c43aca3a474098bd5ca403c3fc.
Strike Maranhao_bf646eec	This strike sends a malware sample known as Maranhao. Maranhao Stealer is a Node.js powered malware of the info-stealer type that targets sensitive user data. It is delivered through phishing emails containing malicious attachments or links. Upon execution, it collects various types of sensitive information including browser data, cryptocurrency wallets, and system information. Its key capabilities include data exfiltration, system information collection, and credential theft from multiple sources such as browsers and cryptocurrency wallets. The MD5 hash of this Maranhao sample is bf646eec3161c66a48001eba3e2772a4.
Strike Maranhao_c9912bd4	This strike sends a malware sample known as Maranhao. Maranhao Stealer is a Node.js powered malware of the info-stealer type that targets sensitive user data. It is delivered through phishing emails containing malicious attachments or links. Upon execution, it collects various types of sensitive information including browser data, cryptocurrency wallets, and system information. Its key capabilities include data exfiltration, system information collection, and credential theft from multiple sources such as browsers and cryptocurrency wallets. The MD5 hash of this Maranhao sample is c9912bd4cb21fa0fc9fc1a0311cb95ed.

<b>Name</b>	<b>Description</b>
Strike Maranhao_dc2ebe2f	This strike sends a malware sample known as Maranhao. Maranhao Stealer is a Node.js powered malware of the info-stealer type that targets sensitive user data. It is delivered through phishing emails containing malicious attachments or links. Upon execution, it collects various types of sensitive information including browser data, cryptocurrency wallets, and system information. Its key capabilities include data exfiltration, system information collection, and credential theft from multiple sources such as browsers and cryptocurrency wallets. The MD5 hash of this Maranhao sample is dc2ebe2fb7935f7b2161dd4eb93d961d.
Strike Maze_07ba093c	This strike sends a malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is 07ba093cb068d944bb37d2818313bd22.
Strike Maze_15b1551e	This strike sends a polymorphic malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The binary has the checksum removed in the PE file format. The MD5 hash of this Maze sample is 15b1551e3f04415a74af35e5313288c0.
Strike Maze_1d746808	This strike sends a malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is 1d74680891b4955ff98287f689d23016.
Strike Maze_2332f770	This strike sends a malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is 2332f770b014f21bcc63c7bee50d543a.
Strike Maze_2dc7d46a	This strike sends a malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is 2dc7d46a099972e5fabcaea4cbcfc3da.

<b>Name</b>	<b>Description</b>
Strike Maze_314d2715	This strike sends a malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is 314d27152364f25a27b57456ee6af2ff.
Strike Maze_35a4ba50	This strike sends a malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is 35a4ba50a7d6aac61fc36980a6153df2.
Strike Maze_5f1ca1b1	This strike sends a polymorphic malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Maze sample is 5f1ca1b153a69bdb23c814540ba0000d.
Strike Maze_64e4ae61	This strike sends a polymorphic malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Maze sample is 64e4ae61550c249b0d4dfb649baa64fc.
Strike Maze_7f152df4	This strike sends a malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is 7f152df418bbb484337fc8ed1383b27d.
Strike Maze_7fdff4b0	This strike sends a polymorphic malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The binary has been packed using upx packer, with the default options. The MD5 hash of this Maze sample is 7fdff4b02371ce3739f8e47f97ad8568.

<b>Name</b>	<b>Description</b>
Strike Maze_910aa498	This strike sends a malware sample known as Maze. Maze malware also known as ChaCha ransomware is known for not only encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is 910aa49813ee4cc7e4fa0074db5e454a.
Strike Maze_a0dc59b0	This strike sends a malware sample known as Maze. Maze malware also known as ChaCha ransomware is known for not only encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is a0dc59b0f4fdf6d4656946865433bcce.
Strike Maze_b2e20c97	This strike sends a polymorphic malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The binary has random bytes appended at the end of the file. The MD5 hash of this Maze sample is b2e20c97cf72558517d227b7adaf8002.
Strike Maze_b9078b6d	This strike sends a malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is b9078b6db33deb83201c8d2ccb3ced4e.
Strike Maze_b93616a1	This strike sends a malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is b93616a1ea4f4a131cc0507e6c789f94.
Strike Maze_bd9838d8	This strike sends a malware sample known as Maze. Maze malware also known as ChaCha ransomware is known for not only encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is bd9838d84fd77205011e8b0c2bd711e0.

<b>Name</b>	<b>Description</b>
Strike Maze_c043c153	This strike sends a malware sample known as Maze. Maze malware also known as ChaCha ransomware is known for not only encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is c043c153237b334df2f2934f7640e802.
Strike Maze_d6e2396d	This strike sends a malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is d6e2396df72ada10e2bbf0f48cb70462.
Strike Maze_f190f9be	This strike sends a malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is f190f9be2a9e5fca00029676722f3e78.
Strike Maze_f83cef2b	This strike sends a malware sample known as Maze. Maze, also known as ChaCha, is ransomware not only known for encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is f83cef2bf33a4d43e58b771e81af3ecc.
Strike Maze_fba4ccb7	This strike sends a malware sample known as Maze. Maze malware also known as ChaCha ransomware is known for not only encrypting files on the targeted system but for releasing stolen victim information to the public if the ransom is not paid. The ransomware has been delivered via several methods including exploits kits, remote desktop connections and phishing emails. This malware also utilizes many anti reversing and analysis features that make examining it much more difficult. The MD5 hash of this Maze sample is fba4ccb7167176990d5a8d24e9505f71.
Strike Meduza Stealer_45f0b444	This strike sends a malware sample known as Meduza Stealer. Meduza Stealer is a browser data stealer malware. It steals login credentials, browsing history, bookmarks, crypto wallets, password manager data, and 2FA extensions. The MD5 hash of this Meduza Stealer sample is 45f0b444f8de5bf28ffc312212935284.
Strike Mimic_01ff843b	This strike sends a malware sample known as Mimic. Mimic is a ransomware that abuses the APIs of the Everything tool to query files to be encrypted. It has the ability to delete shadow copies, disable Windows Defender, terminate applications and services and perform a variety of other functions. The MD5 hash of this Mimic sample is 01ff843b385a9e4d58e4a892fda02fd5.

<b>Name</b>	<b>Description</b>
Strike Mimic_102bd157	This strike sends a malware sample known as Mimic. Mimic is a ransomware that abuses the APIs of the Everything tool to query files to be encrypted. It has the ability to delete shadow copies, disable Windows Defender, terminate applications and services and perform a variety of other functions. The MD5 hash of this Mimic sample is 102bd157676e752d4e9311b5d17f9d5c.
Strike Mimic_1de4fcc8	This strike sends a malware sample known as Mimic. Mimic is a ransomware that abuses the APIs of the Everything tool to query files to be encrypted. It has the ability to delete shadow copies, disable Windows Defender, terminate applications and services and perform a variety of other functions. The MD5 hash of this Mimic sample is 1de4fcc80167b96285656de16f91c7d1.
Strike Mimic_5120980c	This strike sends a malware sample known as Mimic. Mimic is a ransomware that abuses the APIs of the Everything tool to query files to be encrypted. It has the ability to delete shadow copies, disable Windows Defender, terminate applications and services and perform a variety of other functions. The MD5 hash of this Mimic sample is 5120980c01763759fbc8785899809e6a.
Strike Mimic_6a690a6b	This strike sends a malware sample known as Mimic. Mimic is a ransomware that abuses the APIs of the Everything tool to query files to be encrypted. It has the ability to delete shadow copies, disable Windows Defender, terminate applications and services and perform a variety of other functions. The MD5 hash of this Mimic sample is 6a690a6bf79312af5bebc814e99ea84a.
Strike Mimic_8fb35a35	This strike sends a malware sample known as Mimic. Mimic is a ransomware that abuses the APIs of the Everything tool to query files to be encrypted. It has the ability to delete shadow copies, disable Windows Defender, terminate applications and services and perform a variety of other functions. The MD5 hash of this Mimic sample is 8fb35a353978f59bd81e1e605855965e.
Strike Mimic_9e9c2fc8	This strike sends a malware sample known as Mimic. Mimic is a ransomware that abuses the APIs of the Everything tool to query files to be encrypted. It has the ability to delete shadow copies, disable Windows Defender, terminate applications and services and perform a variety of other functions. The MD5 hash of this Mimic sample is 9e9c2fc872e905817c5501d07ef946b1.
Strike Mimic_a16b5846	This strike sends a malware sample known as Mimic. Mimic is a ransomware that abuses the APIs of the Everything tool to query files to be encrypted. It has the ability to delete shadow copies, disable Windows Defender, terminate applications and services and perform a variety of other functions. The MD5 hash of this Mimic sample is a16b58464d8874f358687c49e5d06806.
Strike Mimic_a626eaec	This strike sends a malware sample known as Mimic. Mimic is a ransomware that abuses the APIs of the Everything tool to query files to be encrypted. It has the ability to delete shadow copies, disable Windows Defender, terminate applications and services and perform a variety of other functions. The MD5 hash of this Mimic sample is a626eaec2acc8605825b63e2ca1be83f.
Strike Mimic_ac34ba84	This strike sends a malware sample known as Mimic. Mimic is a ransomware that abuses the APIs of the Everything tool to query files to be encrypted. It has the ability to delete shadow copies, disable Windows Defender, terminate applications and services and perform a variety of other functions. The MD5 hash of this Mimic sample is ac34ba84a5054cd701efad5dd14645c9.

<b>Name</b>	<b>Description</b>
Strike Mimic_b92a2606	This strike sends a malware sample known as Mimic. Mimic is a ransomware that abuses the APIs of the Everything tool to query files to be encrypted. It has the ability to delete shadow copies, disable Windows Defender, terminate applications and services and perform a variety of other functions. The MD5 hash of this Mimic sample is b92a26068ba3653d8ec491f9702843e7.
Strike Mimic_bc78159e	This strike sends a malware sample known as Mimic. Mimic is a ransomware that abuses the APIs of the Everything tool to query files to be encrypted. It has the ability to delete shadow copies, disable Windows Defender, terminate applications and services and perform a variety of other functions. The MD5 hash of this Mimic sample is bc78159e7368ca429fcba29e97fc4da6.
Strike Mimic_db21ed7d	This strike sends a malware sample known as Mimic. Mimic is a ransomware that abuses the APIs of the Everything tool to query files to be encrypted. It has the ability to delete shadow copies, disable Windows Defender, terminate applications and services and perform a variety of other functions. The MD5 hash of this Mimic sample is db21ed7d19149a615d7432aca9c8f6ca.
Strike Minibike_01cbadd	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is 01cbadd7a269521bf7b80f4a9a1982f.
Strike Minibike_054c6723	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is 054c67236a86d9ab5ec80e16b884f733.
Strike Minibike_2c4cdc0e	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is 2c4cdc0e78ef57b44f11f7ec2f6164cd.
Strike Minibike_3b658afa	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is 3b658afa91ce3327dbfa1cf665529a6d.
Strike Minibike_409c2ac7	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is 409c2ac789015e76f9886f1203a73bc0.
Strike Minibike_664cfda4	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is 664cfda4ada6f8b7bb25a5f50cccf984.

<b>Name</b>	<b>Description</b>
Strike Minibike_68f6810f	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is 68f6810f248d032bbb65b391cdb1d5e0.
Strike Minibike_691d0143	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is 691d0143c0642ff783909f983ccb8ffd.
Strike Minibike_710d1a8b	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is 710d1a8b2fc17c381a7f20da5d2d70fc.
Strike Minibike_75d2c686	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is 75d2c686d410ec1f880a6fd7a9800055.
Strike Minibike_909a235a	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is 909a235ac0349041b38d84e9aab3f3a1.
Strike Minibike_adef679c	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is adef679c6aa6860aa89b775dceb6958b.
Strike Minibike_bfd024e6	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is bfd024e64867e6ca44738dd03d4f87b5.
Strike Minibike_c12ff86d	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is c12ff86d32bd10c6c764b71728a51bce.
Strike Minibike_cf32d73c	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is cf32d73c501d5924b3c98383f53fda51.

<b>Name</b>	<b>Description</b>
Strike Minibike_d94ffe66	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is d94ffe668751935b19eaeb93fed1cdbe.
Strike Minibike_e3dc8810	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is e3dc8810da71812b860fc59aeadcc350.
Strike Minibike_e9ed595b	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is e9ed595b24a7eeb34ac52f57eec6e2b.
Strike Minibike_eadbaabe	This strike sends a malware sample known as Minibike. Minibike is a backdoor that performs directory and file enumeration, exfiltration, upload, and command execution. The malware uses the Azure cloud infrastructure for command and control communication. The MD5 hash of this Minibike sample is eadbaabe3b8133426bcf09f7102088d4.
Strike Minibus_05fcace6	This strike sends a malware sample known as Minibus. Minibus similar to the closely related Minibike malware is a backdoor that has a command interface and advanced reconnaissance features. It includes features like process enumeration and performs command and control communication utilizing a combination of Azure cloud infrastructure and .com domains. The MD5 hash of this Minibus sample is 05fcace605b525f1bece1813bb18a56c.
Strike Minibus_4ed5d74a	This strike sends a malware sample known as Minibus. Minibus similar to the closely related Minibike malware is a backdoor that has a command interface and advanced reconnaissance features. It includes features like process enumeration and performs command and control communication utilizing a combination of Azure cloud infrastructure and .com domains. The MD5 hash of this Minibus sample is 4ed5d74a746461d3faa9f96995a1eec8.
Strike Minibus_816af741	This strike sends a malware sample known as Minibus. Minibus similar to the closely related Minibike malware is a backdoor that has a command interface and advanced reconnaissance features. It includes features like process enumeration and performs command and control communication utilizing a combination of Azure cloud infrastructure and .com domains. The MD5 hash of this Minibus sample is 816af741c3d6be1397d306841d12e206.
Strike Minibus_c5dc2c75	This strike sends a malware sample known as Minibus. Minibus similar to the closely related Minibike malware is a backdoor that has a command interface and advanced reconnaissance features. It includes features like process enumeration and performs command and control communication utilizing a combination of Azure cloud infrastructure and .com domains. The MD5 hash of this Minibus sample is c5dc2c75459dc99a42400f6d8b455250.

<b>Name</b>	<b>Description</b>
Strike Minibus_f58e0dfb	This strike sends a malware sample known as Minibus. Minibus similar to the closely related Minibike malware is a backdoor that has a command interface and advanced reconnaissance features. It includes features like process enumeration and performs command and control communication utilizing a combination of Azure cloud infrastructure and .com domains. The MD5 hash of this Minibus sample is f58e0dfb8f915fa5ce1b7ca50c46b51b.
Strike Mirai TBOT_013183e9	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is 013183e99a5ca41e36da2bf5a1d4ad5e.
Strike Mirai TBOT_0f98a0c5	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is 0f98a0c5a171e4b76504c1364744e21d.
Strike Mirai TBOT_1ce7682e	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is 1ce7682e9f661823bf5227f32a5d994f.
Strike Mirai TBOT_2dbd24f9	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is 2dbd24f9bec506e7f588bcb5939066d1.
Strike Mirai TBOT_397143ff	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is 397143ff0e9473c0d9325b54e47db40d.
Strike Mirai TBOT_401d2428	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is 401d24286653075ef5fe54534c2db798.

<b>Name</b>	<b>Description</b>
Strike Mirai TBOT_625db875	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is 625db8751696ad3b14e07fc4ee787f80.
Strike Mirai TBOT_6801e817	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is 6801e8171e4090b3f9b1c6b6f3af869f.
Strike Mirai TBOT_6ceb3256	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is 6ceb32565788fdaff114965b896ef17e.
Strike Mirai TBOT_6fb1e7cd	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is 6fb1e7cdff0485801a16381519ada0bd.
Strike Mirai TBOT_8c8d6253	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is 8c8d6253a907a75518b7f37ac4fb5c75.
Strike Mirai TBOT_9bd95828	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is 9bd95828aa90d7cfbc36e85fa77b7088.
Strike Mirai TBOT_9d78eb3d	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is 9d78eb3d2db7feca788d0d361662f977.

<b>Name</b>	<b>Description</b>
Strike Mirai TBOT_b89519b2	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is b89519b2a2cadd6e77bd1ee219d459e7.
Strike Mirai TBOT_b8ace535	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is b8ace535bb02910ef0f5db3d2575e2a0.
Strike Mirai TBOT_bbc6bd3a	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is bbc6bd3a07fad7c2412a1484022eaa01.
Strike Mirai TBOT_c81c380e	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is c81c380ec4b0273f937e4f1a1799d44d.
Strike Mirai TBOT_cffa7820	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is cffa78205ab5ea75fe051b32c5297bd1.
Strike Mirai TBOT_de0eb825	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is de0eb825f0bce40296089a12810eddb6.
Strike Mirai TBOT_ebf1a637	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is ebf1a637e7c45e96da5c9382562d850d.

<b>Name</b>	<b>Description</b>
Strike Mirai TBOT_f3dd2282	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is f3dd22821a86cd9f91c01bb30286cc85.
Strike Mirai TBOT_f88fd951	This strike sends a malware sample known as Mirai TBOT. Mirai.TBOT is a sophisticated Mirai botnet distinguished by its extensive use of over 100 bot groups, each employing unique infection methods. It possesses the capability to exploit zero-day vulnerabilities and utilizes OpenNIC custom C2 domains. The botnet operates on a massive scale and is primarily employed for DDoS attacks. The MD5 hash of this Mirai TBOT sample is f88fd951081f09617d5703ccefc5d356.
Strike Mispadu MSI_1a03283c	This strike sends a malware sample known as Mispadu MSI. Mispadu also known as Ursu is a banking trojan that uses phishing emails in order to exfiltrate sensitive credentials. First the email contains a pdf that lures the victim to initiate a download of a zip file that contains an MSI installer or HTA script. The execution of these eventually lead to the download and execution of a couple VBScripts and finally an AutoIT script that loads a dll into memory. The main payload extracts browser and email client credentials. This sample is the MSI. The MD5 hash of this Mispadu MSI sample is 1a03283cca237aed77a57229b69fd4c8.
Strike Mispadu MSI_2ddc9977	This strike sends a malware sample known as Mispadu MSI. Mispadu also known as Ursu is a banking trojan that uses phishing emails in order to exfiltrate sensitive credentials. First the email contains a pdf that lures the victim to initiate a download of a zip file that contains an MSI installer or HTA script. The execution of these eventually lead to the download and execution of a couple VBScripts and finally an AutoIT script that loads a dll into memory. The main payload extracts browser and email client credentials. This sample is the MSI. The MD5 hash of this Mispadu MSI sample is 2ddc997762f32dd0ad3ca4771d39dbd7.
Strike Mispadu MSI_40453db5	This strike sends a malware sample known as Mispadu MSI. Mispadu also known as Ursu is a banking trojan that uses phishing emails in order to exfiltrate sensitive credentials. First the email contains a pdf that lures the victim to initiate a download of a zip file that contains an MSI installer or HTA script. The execution of these eventually lead to the download and execution of a couple VBScripts and finally an AutoIT script that loads a dll into memory. The main payload extracts browser and email client credentials. This sample is the MSI. The MD5 hash of this Mispadu MSI sample is 40453db553c3656c9083179361cf4765.
Strike Mispadu MSI_540118ed	This strike sends a malware sample known as Mispadu MSI. Mispadu also known as Ursu is a banking trojan that uses phishing emails in order to exfiltrate sensitive credentials. First the email contains a pdf that lures the victim to initiate a download of a zip file that contains an MSI installer or HTA script. The execution of these eventually lead to the download and execution of a couple VBScripts and finally an AutoIT script that loads a dll into memory. The main payload extracts browser and email client credentials. This sample is the MSI. The MD5 hash of this Mispadu MSI sample is 540118ed71408b7bc31049ffd807086f.

<b>Name</b>	<b>Description</b>
Strike Mispadu MSI_6a449567	This strike sends a malware sample known as Mispadu MSI. Mispadu also known as Ursu is a banking trojan that uses phishing emails in order to exfiltrate sensitive credentials. First the email contains a pdf that lures the victim to initiate a download of a zip file that contains an MSI installer or HTA script. The execution of these eventually lead to the download and execution of a couple VBScripts and finally an AutoIT script that loads a dll into memory. The main payload extracts browser and email client credentials. This sample is the MSI. The MD5 hash of this Mispadu MSI sample is 6a449567f353dce7cfef5bc10c334655.
Strike Mispadu MSI_6bfcfddf	This strike sends a malware sample known as Mispadu MSI. Mispadu also known as Ursu is a banking trojan that uses phishing emails in order to exfiltrate sensitive credentials. First the email contains a pdf that lures the victim to initiate a download of a zip file that contains an MSI installer or HTA script. The execution of these eventually lead to the download and execution of a couple VBScripts and finally an AutoIT script that loads a dll into memory. The main payload extracts browser and email client credentials. This sample is the MSI. The MD5 hash of this Mispadu MSI sample is 6bfcfdd1c04f07adfea18227857e5cf.
Strike Mispadu MSI_7acf4aed	This strike sends a malware sample known as Mispadu MSI. Mispadu also known as Ursu is a banking trojan that uses phishing emails in order to exfiltrate sensitive credentials. First the email contains a pdf that lures the victim to initiate a download of a zip file that contains an MSI installer or HTA script. The execution of these eventually lead to the download and execution of a couple VBScripts and finally an AutoIT script that loads a dll into memory. The main payload extracts browser and email client credentials. This sample is the MSI. The MD5 hash of this Mispadu MSI sample is 7acf4aed2fb50d6de5b0f57302070b88.
Strike Mispadu MSI_8027bb46	This strike sends a malware sample known as Mispadu MSI. Mispadu also known as Ursu is a banking trojan that uses phishing emails in order to exfiltrate sensitive credentials. First the email contains a pdf that lures the victim to initiate a download of a zip file that contains an MSI installer or HTA script. The execution of these eventually lead to the download and execution of a couple VBScripts and finally an AutoIT script that loads a dll into memory. The main payload extracts browser and email client credentials. This sample is the MSI. The MD5 hash of this Mispadu MSI sample is 8027bb46ec1892abe98bb0d18902d93a.
Strike Mispadu MSI_c1353d21	This strike sends a malware sample known as Mispadu MSI. Mispadu also known as Ursu is a banking trojan that uses phishing emails in order to exfiltrate sensitive credentials. First the email contains a pdf that lures the victim to initiate a download of a zip file that contains an MSI installer or HTA script. The execution of these eventually lead to the download and execution of a couple VBScripts and finally an AutoIT script that loads a dll into memory. The main payload extracts browser and email client credentials. This sample is the MSI. The MD5 hash of this Mispadu MSI sample is c1353d2194f2ae2ecf5f82434137c426.

<b>Name</b>	<b>Description</b>
Strike Mispadu PDF_238e4731	This strike sends a malware sample known as Mispadu PDF. Mispadu also known as Ursu is a banking trojan that uses phishing emails in order to exfiltrate sensitive credentials. First the email contains a pdf that lures the victim to initiate a download of a zip file that contains an MSI installer or HTA script. The execution of these eventually lead to the download and execution of a couple VBScripts and finally an AutoIT script that loads a dll into memory. The main payload extracts browser and email client credentials. This sample is the initial pdf. The MD5 hash of this Mispadu PDF sample is 238e4731b4d05011ccec45ccc28c6c7b.
Strike Mispadu PDF_3b307fac	This strike sends a malware sample known as Mispadu PDF. Mispadu also known as Ursu is a banking trojan that uses phishing emails in order to exfiltrate sensitive credentials. First the email contains a pdf that lures the victim to initiate a download of a zip file that contains an MSI installer or HTA script. The execution of these eventually lead to the download and execution of a couple VBScripts and finally an AutoIT script that loads a dll into memory. The main payload extracts browser and email client credentials. This sample is the initial pdf. The MD5 hash of this Mispadu PDF sample is 3b307facf2b5e411f05159fbedabc3bf.
Strike Mispadu VBS_15465965	This strike sends a malware sample known as Mispadu VBS. Mispadu also known as Ursu is a banking trojan that uses phishing emails in order to exfiltrate sensitive credentials. First the email contains a pdf that lures the victim to initiate a download of a zip file that contains an MSI installer or HTA script. The execution of these eventually lead to the download and execution of a couple VBScripts and finally an AutoIT script that loads a dll into memory. The main payload extracts browser and email client credentials. This sample is the VBScript. The MD5 hash of this Mispadu VBS sample is 1546596599992042b708d99c5bc1e7d1.
Strike Mispadu VBS_52a21157	This strike sends a malware sample known as Mispadu VBS. Mispadu also known as Ursu is a banking trojan that uses phishing emails in order to exfiltrate sensitive credentials. First the email contains a pdf that lures the victim to initiate a download of a zip file that contains an MSI installer or HTA script. The execution of these eventually lead to the download and execution of a couple VBScripts and finally an AutoIT script that loads a dll into memory. The main payload extracts browser and email client credentials. This sample is the VBScript. The MD5 hash of this Mispadu VBS sample is 52a21157625540fb8b36e8e255da5f17.
Strike Mispadu VBS_8c1008f3	This strike sends a malware sample known as Mispadu VBS. Mispadu also known as Ursu is a banking trojan that uses phishing emails in order to exfiltrate sensitive credentials. First the email contains a pdf that lures the victim to initiate a download of a zip file that contains an MSI installer or HTA script. The execution of these eventually lead to the download and execution of a couple VBScripts and finally an AutoIT script that loads a dll into memory. The main payload extracts browser and email client credentials. This sample is the VBScript. The MD5 hash of this Mispadu VBS sample is 8c1008f32fe21a9953cbaae74e3933a8.
Strike MoonPeak_1c80fb45	This strike sends a malware sample known as MoonPeak. MoonPeak is a remote access trojan based off of the XenoRAT family of malware. It has been attributed to the North Korean state sponsored group known as UAT-5394. It contains many of the same capabilities as XenoRAT such as key logging and information gathering. It sends this data back to the attacker controlled C2. The MD5 hash of this MoonPeak sample is 1c80fb45a89106369e1b47b1b0ccb38a.

<b>Name</b>	<b>Description</b>
Strike MoonPeak_2a40543f	This strike sends a malware sample known as MoonPeak. MoonPeak is a remote access trojan based off of the XenoRAT family of malware. It has been attributed to the North Korean state sponsored group known as UAT-5394. It contains many of the same capabilities as XenoRAT such as key logging and information gathering. It sends this data back to the attacker controlled C2. The MD5 hash of this MoonPeak sample is 2a40543f5b4b8cc1f4bd8993df44708e.
Strike MoonPeak_3c8ce3a7	This strike sends a malware sample known as MoonPeak. MoonPeak is a remote access trojan based off of the XenoRAT family of malware. It has been attributed to the North Korean state sponsored group known as UAT-5394. It contains many of the same capabilities as XenoRAT such as key logging and information gathering. It sends this data back to the attacker controlled C2. The MD5 hash of this MoonPeak sample is 3c8ce3a7ac8ef626f10c8128e5892f0b.
Strike MoonPeak_535f59bc	This strike sends a malware sample known as MoonPeak. MoonPeak is a remote access trojan based off of the XenoRAT family of malware. It has been attributed to the North Korean state sponsored group known as UAT-5394. It contains many of the same capabilities as XenoRAT such as key logging and information gathering. It sends this data back to the attacker controlled C2. The MD5 hash of this MoonPeak sample is 535f59bc95fe3efc22abf5036c60ade0.
Strike MoonPeak_571c5775	This strike sends a malware sample known as MoonPeak. MoonPeak is a remote access trojan based off of the XenoRAT family of malware. It has been attributed to the North Korean state sponsored group known as UAT-5394. It contains many of the same capabilities as XenoRAT such as key logging and information gathering. It sends this data back to the attacker controlled C2. The MD5 hash of this MoonPeak sample is 571c577595223518fd5a3ee8b36928d7.
Strike MoonPeak_60e8ed6c	This strike sends a malware sample known as MoonPeak. MoonPeak is a remote access trojan based off of the XenoRAT family of malware. It has been attributed to the North Korean state sponsored group known as UAT-5394. It contains many of the same capabilities as XenoRAT such as key logging and information gathering. It sends this data back to the attacker controlled C2. The MD5 hash of this MoonPeak sample is 60e8ed6c37e1fe9742a49916e07002e5.
Strike MoonPeak_9924b244	This strike sends a malware sample known as MoonPeak. MoonPeak is a remote access trojan based off of the XenoRAT family of malware. It has been attributed to the North Korean state sponsored group known as UAT-5394. It contains many of the same capabilities as XenoRAT such as key logging and information gathering. It sends this data back to the attacker controlled C2. The MD5 hash of this MoonPeak sample is 9924b24434e2d92d0fc3b683006cbad1.
Strike MoonPeak_a470afe2	This strike sends a malware sample known as MoonPeak. MoonPeak is a remote access trojan based off of the XenoRAT family of malware. It has been attributed to the North Korean state sponsored group known as UAT-5394. It contains many of the same capabilities as XenoRAT such as key logging and information gathering. It sends this data back to the attacker controlled C2. The MD5 hash of this MoonPeak sample is a470afe2f7176694553158bcd3decb53.
Strike MoonPeak_ca005ebe	This strike sends a malware sample known as MoonPeak. MoonPeak is a remote access trojan based off of the XenoRAT family of malware. It has been attributed to the North Korean state sponsored group known as UAT-5394. It contains many of the same capabilities as XenoRAT such as key logging and information gathering. It sends this data back to the attacker controlled C2. The MD5 hash of this MoonPeak sample is ca005ebe9454f30c2cedd73080677f56.

<b>Name</b>	<b>Description</b>
Strike MoonPeak_d3dd07f2	This strike sends a malware sample known as MoonPeak. MoonPeak is a remote access trojan based off of the XenoRAT family of malware. It has been attributed to the North Korean state sponsored group known as UAT-5394. It contains many of the same capabilities as XenoRAT such as key logging and information gathering. It sends this data back to the attacker controlled C2. The MD5 hash of this MoonPeak sample is d3dd07f2454b9c81d9d16e65d6f24000.
Strike MoonPeak_dd4ca3ea	This strike sends a malware sample known as MoonPeak. MoonPeak is a remote access trojan based off of the XenoRAT family of malware. It has been attributed to the North Korean state sponsored group known as UAT-5394. It contains many of the same capabilities as XenoRAT such as key logging and information gathering. It sends this data back to the attacker controlled C2. The MD5 hash of this MoonPeak sample is dd4ca3ea5c13241be3cc4f7f64a7c05c.
Strike MoonPeak_e8ab7a58	This strike sends a malware sample known as MoonPeak. MoonPeak is a remote access trojan based off of the XenoRAT family of malware. It has been attributed to the North Korean state sponsored group known as UAT-5394. It contains many of the same capabilities as XenoRAT such as key logging and information gathering. It sends this data back to the attacker controlled C2. The MD5 hash of this MoonPeak sample is e8ab7a58f35cae486d61c94910faa4fa.
Strike MoonPeak_ee1dca47	This strike sends a malware sample known as MoonPeak. MoonPeak is a remote access trojan based off of the XenoRAT family of malware. It has been attributed to the North Korean state sponsored group known as UAT-5394. It contains many of the same capabilities as XenoRAT such as key logging and information gathering. It sends this data back to the attacker controlled C2. The MD5 hash of this MoonPeak sample is ee1dca47840fbab6d8956ef97f352496.
Strike MoonPeak_fcfc07e5	This strike sends a malware sample known as MoonPeak. MoonPeak is a remote access trojan based off of the XenoRAT family of malware. It has been attributed to the North Korean state sponsored group known as UAT-5394. It contains many of the same capabilities as XenoRAT such as key logging and information gathering. It sends this data back to the attacker controlled C2. The MD5 hash of this MoonPeak sample is fcfc07e56f496e836c29833b89a23fce.
Strike Moqhao_2e7acc13	This strike sends an Android malware sample known as Moqhao. It is attributed to the Yanbian Gang and is a descendant of the Roaming Mantis malware family. The sample poses as an update of the Chrome application and is spread through smishing attacks. It is known to target wireless routers bypassing security CAPTCHAs to perform DNS hijacking attacks leading the victims to other malicious websites. 'zfi.kkvwej.cby.hpyz' is the package name of the malware sample. The MD5 hash of this Moqhao sample is 2e7acc13e9a9911cb5dd4057c5f0c343.
Strike Moqhao_391b0462	This strike sends an Android polymorphic malware sample known as Moqhao. It is attributed to the Yanbian Gang and is a descendant of the Roaming Mantis malware family. The sample poses as an update of the Chrome application and is spread through smishing attacks. It is known to target wireless routers bypassing security CAPTCHAs to perform DNS hijacking attacks leading the victims to other malicious websites. 'zfi.kkvwej.cby.hpyz' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this Moqhao sample is 391b0462e9b775f10ef9b52132620ecf.

<b>Name</b>	<b>Description</b>
Strike Moqhao_6b3a51e0	<p>This strike sends an Android polymorphic malware sample known as Moqhao. It is attributed to the Yanbian Gang and is a descendant of the Roaming Mantis malware family. The sample poses as an update of the Chrome application and is spread through smishing attacks. It is known to target wireless routers bypassing security CAPTCHAs to perform DNS hijacking attacks leading the victims to other malicious websites. 'zfi.kkvwej.cby.hpyz' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this Moqhao sample is 6b3a51e03c95c659566774757a963745.</p>
Strike MrAnon Stealer_00429bb3	<p>This strike sends a malware sample known as MrAnon Stealer. MrAnon Stealer is a Python-based information-stealing malware. Attacker disguises as a hotel reservation inquiry and sends deceptive emails containing a malicious PDF file. Upon opening, the PDF downloads a .NET executable file created with PowerGUI, initiating a PowerShell script execution to deploy MrAnon Stealer. This malware is compressed with cx-Freeze to evade detection, targets victims primarily in Germany. MrAnon Stealer is designed to exfiltrate sensitive information, including credentials, system details, browser sessions, and cryptocurrency-related data. The MD5 hash of this MrAnon Stealer sample is 00429bb31985145568e6f62171047e0b.</p>
Strike MrAnon Stealer_717d5a61	<p>This strike sends a malware sample known as MrAnon Stealer. MrAnon Stealer is a Python-based information-stealing malware. Attacker disguises as a hotel reservation inquiry and sends deceptive emails containing a malicious PDF file. Upon opening, the PDF downloads a .NET executable file created with PowerGUI, initiating a PowerShell script execution to deploy MrAnon Stealer. This malware is compressed with cx-Freeze to evade detection, targets victims primarily in Germany. MrAnon Stealer is designed to exfiltrate sensitive information, including credentials, system details, browser sessions, and cryptocurrency-related data. The MD5 hash of this MrAnon Stealer sample is 717d5a612325dc5c620e457587f7a0c7.</p>
Strike MrAnon Stealer_822dff83	<p>This strike sends a malware sample known as MrAnon Stealer. MrAnon Stealer is a Python-based information-stealing malware. Attacker disguises as a hotel reservation inquiry and sends deceptive emails containing a malicious PDF file. Upon opening, the PDF downloads a .NET executable file created with PowerGUI, initiating a PowerShell script execution to deploy MrAnon Stealer. This malware is compressed with cx-Freeze to evade detection, targets victims primarily in Germany. MrAnon Stealer is designed to exfiltrate sensitive information, including credentials, system details, browser sessions, and cryptocurrency-related data. The MD5 hash of this MrAnon Stealer sample is 822dff83502fc6d04884572a354aeab9.</p>
Strike MrAnon Stealer_b41f639f	<p>This strike sends a malware sample known as MrAnon Stealer. MrAnon Stealer is a Python-based information-stealing malware. Attacker disguises as a hotel reservation inquiry and sends deceptive emails containing a malicious PDF file. Upon opening, the PDF downloads a .NET executable file created with PowerGUI, initiating a PowerShell script execution to deploy MrAnon Stealer. This malware is compressed with cx-Freeze to evade detection, targets victims primarily in Germany. MrAnon Stealer is designed to exfiltrate sensitive information, including credentials, system details, browser sessions, and cryptocurrency-related data. The MD5 hash of this MrAnon Stealer sample is b41f639f652edfda7b6d2e59f9947b99.</p>

<b>Name</b>	<b>Description</b>
Strike MuddyC2Go_22971759	<p>This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is 22971759adf816c6fb43104c0e1d89d6.</p>
Strike MuddyC2Go_245c3ed3	<p>This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is 245c3ed373727c21ad9ee862b767e362.</p>
Strike MuddyC2Go_34212eb9	<p>This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is 34212eb9e2af84eceb6a8234d28751b6.</p>
Strike MuddyC2Go_3c6486df	<p>This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is 3c6486dfb691fc6642f1d35bdf247b90.</p>

<b>Name</b>	<b>Description</b>
Strike MuddyC2Go_4a70b1e4	<p>This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is 4a70b1e4cb57c99502d89cdbbed48343.</p>
Strike MuddyC2Go_55b99af8	<p>This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is 55b99af81610eb65aabea796130a0462.</p>
Strike MuddyC2Go_57641ce5	<p>This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is 57641ce5af4482038c9ea27afcc087ee.</p>
Strike MuddyC2Go_79a638b2	<p>This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is 79a638b2f2cc82bfe137f1d12534cda5.</p>

<b>Name</b>	<b>Description</b>
Strike MuddyC2Go_99572509	<p>This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is 9957250940377b39e405114f0a2fe84b.</p>
Strike MuddyC2Go_b867ec1c	<p>This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is b867ec1cef6b1618a21853fb8cafd6e1.</p>
Strike MuddyC2Go_d3a2dee3	<p>This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is d3a2dee3bb8fcda8e8a0d404e7d1e6efb.</p>
Strike MuddyC2Go_d7ca8f3b	<p>This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is d7ca8f3b5e21ed56abf32ac7cb158a7e.</p>

Name	Description
Strike MuddyC2Go_db0e68d7	This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is db0e68d7d81f5c21e6e458445fd6e34b.
Strike MuddyC2Go_dbcc0e9c	This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is dbcc0e9c1c6c1fff790caa0b2ffc2fe5.
Strike MuddyC2Go_e07adc4e	This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is e07adc4ee768126dc7c7339f4cb00120.
Strike MuddyC2Go_f08aa714	This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is f08aa714fd59b68924843cbfddac4b15.

<b>Name</b>	<b>Description</b>
Strike MuddyC2Go_fc523904	<p>This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is fc523904ca6e191eb2fdb254a6225577.</p>
Strike MuddyC2Go_fe5f94e5	<p>This strike sends a malware sample known as MuddyC2Go. MuddyC2Go is a Command and Control (C2) framework utilized by the MuddyWater Advanced Persistent Threat (APT). This framework's web component is coded in Go, distinguishing it from its predecessor PhonyC2. MuddyWater utilizes spear phishing emails with password-protected archives and executables to spread its malicious payloads. This executable contains an embedded PowerShell script that automatically connects to MuddyWater's C2, eliminating the need for manual execution by attackers. The response from the C2 is also a PowerShell script that runs every 10 seconds and waits for commands from the attacker using the C2. The MD5 hash of this MuddyC2Go sample is fe5f94e5df19d95df26aaf774daad9df.</p>
Strike Murdoc Botnet_001ba5bc	<p>This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 001ba5bcd535088c420d5a7cc8a2e70e.</p>
Strike Murdoc Botnet_0142d1ae	<p>This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 0142d1ae25f6c186173fd7be20ab0d35.</p>
Strike Murdoc Botnet_0637b9df	<p>This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 0637b9df9d6938f48d959e1697d4ef81.</p>
Strike Murdoc Botnet_0e1e28fd	<p>This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 0e1e28fda71c433d734539538e5f5d1a.</p>

<b>Name</b>	<b>Description</b>
Strike Murdoc Botnet_0fe4f0fb	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 0fe4f0fb4c4ca8e779a19c6d0f07db68.
Strike Murdoc Botnet_16809129	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 16809129d70e2086b48500d544ea8d41.
Strike Murdoc Botnet_1f7529e7	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 1f7529e735437f949cb531228ee3d353.
Strike Murdoc Botnet_23ee5a8b	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 23ee5a8b998de681eb94885abdb35dd6.
Strike Murdoc Botnet_26422beb	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 26422bebe81def0c3bae25946427f78d.
Strike Murdoc Botnet_2bc99a01	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 2bc99a018da0650c9bc0fa56c7c79320.
Strike Murdoc Botnet_2c5a74ff	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 2c5a74ff1dadea587b0f61b8217ffa33.
Strike Murdoc Botnet_32136787	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 321367874c11451a5ac8f89551cdf5a7.

<b>Name</b>	<b>Description</b>
Strike Murdoc Botnet_344202a7	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 344202a75c93c712af47bf0c865b38f4.
Strike Murdoc Botnet_34f2a08c	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 34f2a08c8be4b9dd28b68ec8f74db905.
Strike Murdoc Botnet_37e97a09	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 37e97a09ba3e7255c3ce289dc4c951d3.
Strike Murdoc Botnet_54bc7ded	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 54bc7ded42ad84c533b2559df52fe9ed.
Strike Murdoc Botnet_5bf7742d	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 5bf7742d8a20a9ccbd7af5a4cad4fb4a.
Strike Murdoc Botnet_6966fbfd	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 6966fbfdf73a15dc33e3cf857be7dd61.
Strike Murdoc Botnet_6d459d0c	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 6d459d0c0617fd1d907a1703f7d05774.
Strike Murdoc Botnet_769aea7e	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 769aea7ea26bfc99dd337dbb26191705.

<b>Name</b>	<b>Description</b>
Strike Murdoc Botnet_76abe173	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 76abe173655108323199f1f3df7cdc6e.
Strike Murdoc Botnet_7d44dcdd	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 7d44dcddfb7b57c777ffa55aae9c2427.
Strike Murdoc Botnet_802ea211	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 802ea21155b88f73bf835d044c6999c3.
Strike Murdoc Botnet_8bed0b9a	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 8bed0b9a5fcf46fdc9d31a669a3f99be.
Strike Murdoc Botnet_940f6c62	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is 940f6c62564d6e8c510f592ae6f7c5b7.
Strike Murdoc Botnet_a9d06491	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is a9d06491667aa1b1779a05d2d155f53b.
Strike Murdoc Botnet_b5a042a7	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is b5a042a7f1031583a2e2561aa9bb42f5.
Strike Murdoc Botnet_e1ec05d0	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is e1ec05d07d1a1527ecc04b4cf910be67.

<b>Name</b>	<b>Description</b>
Strike Murdoc Botnet_ef012ac9	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is ef012ac99eec265ae35280145217eafb.
Strike Murdoc Botnet_f8cb1314	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is f8cb13149c23bbd473d188a22895da3b.
Strike Murdoc Botnet_fa25a367	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is fa25a367264bf80241953c025c172fde.
Strike Murdoc Botnet_fc453786	This strike sends a malware sample known as Murdoc Botnet. Murdoc Botnet is a large scale attack that is considered a variant of the Mirai campaign. It exploits vulnerabilities targeting AVTECH Cameras and Huawei routers. The botnet uses embedded exploits to download additional payloads to then install on the infected devices. The MD5 hash of this Murdoc Botnet sample is fc453786c874149e665953b442ae9594.
Strike NOOPLDR_213f4f64	This strike sends a malware sample known as NOOPLDR. NOOPLDR is a malware that is associated with the MirrorFace threat group. It is the malware loader that gets executed after the NOOPDOOR shellcode is executed. NOOPLDR is loaded via DLL side-loading to a legitimate Windows application. It loads the registry and injects decrypted code into this application. After NOOPDOOR executes, the loader encrypts the code stored in a preset registry so next time it runs, it can be loaded. The MD5 hash of this NOOPLDR sample is 213f4f64aa92b5cc06c2f38bd28f0d6c.
Strike NOOPLDR_4f1c68d2	This strike sends a malware sample known as NOOPLDR. NOOPLDR is a malware that is associated with the MirrorFace threat group. It is the malware loader that gets executed after the NOOPDOOR shellcode is executed. NOOPLDR is loaded via DLL side-loading to a legitimate Windows application. It loads the registry and injects decrypted code into this application. After NOOPDOOR executes, the loader encrypts the code stored in a preset registry so next time it runs, it can be loaded. The MD5 hash of this NOOPLDR sample is 4f1c68d2fe3b0255e706e4c7de0a739f.
Strike Nanocore_0df610ea	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 0df610eaf1432e0b18aa27e4eabc931a.

<b>Name</b>	<b>Description</b>
Strike Nanocore_0e643852	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 0e643852c47f9850cc74bf5cdcc59291.
Strike Nanocore_1a74354a	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 1a74354aa911475d3787eb9f63a57acd.
Strike Nanocore_1f9b44c9	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 1f9b44c987c087f9ac0df45510701795.
Strike Nanocore_2e2dfbb1	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 2e2dfbb18adceb71d6785790792b5fd5.
Strike Nanocore_343a00e0	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 343a00e0236966f55dcd7f7793821ea3.
Strike Nanocore_38cee96e	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 38cee96e344836bcf081a164e1499cd8.
Strike Nanocore_3b72cad1	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 3b72cad1541f9f0e9723c7b6b462cfb3.
Strike Nanocore_5345f05c	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 5345f05c846bcec9128116d080cc8aa8.
Strike Nanocore_5d1b8c65	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 5d1b8c65e931124a25d4b51f0b5a3562.

<b>Name</b>	<b>Description</b>
Strike Nanocore_5fd23435	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 5fd23435c94a809ec2351a44137fcbfc.
Strike Nanocore_656265f4	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 656265f4773e9fce528b9dd1d3685c5f.
Strike Nanocore_677d8f9d	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 677d8f9dc4f65fd974e3df7d579d2205.
Strike Nanocore_6a98fe51	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 6a98fe519e79a71d03da47d2ae68d529.
Strike Nanocore_818a1477	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 818a1477cbbdf0888524352ff075e68f.
Strike Nanocore_87bb61d6	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 87bb61d698092811de9c9608eb3535fb.
Strike Nanocore_8b4b1d7c	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 8b4b1d7c42d2db7f3a5ccb826ab1c894.
Strike Nanocore_8c38d68a	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 8c38d68a667c25d9688350f6e6d483ee.
Strike Nanocore_97531e3a	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 97531e3a2e53b602f0fe470d0080f568.

<b>Name</b>	<b>Description</b>
Strike Nanocore_9fdc8981	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is 9fdc898122e5048dd40054608952290c.
Strike Nanocore_a7755817	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is a775581737895ae440ada6d5eb68f1b4.
Strike Nanocore_beb5e37d	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is beb5e37de290abb7ad40624b67ffe93a.
Strike Nanocore_c24e32e2	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is c24e32e2f5e4dcd95f76722619b1c0a1.
Strike Nanocore_d8661f7d	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is d8661f7d65f4a2123b5257131c8ba54c.
Strike Nanocore_daab0fb9	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is daab0fbde90d733f89e781e6613a88e6.
Strike Nanocore_f100541a	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is f100541afa58ccf5a261829e822f9a36.
Strike Nanocore_f28a8791	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is f28a87919c239a05f71658d8708548fd.
Strike Nanocore_fbfb66e	This strike sends a malware sample known as Nanocore. Nanocore is a .NET Remote Access Trojan. It has become widely available. This trojan has many capabilities including monitoring the system audio and video, controlling the desktop, and logging the user's keystrokes. The MD5 hash of this Nanocore sample is fbfb66e81bbbd6156f6c62a5b5ee138.

<b>Name</b>	<b>Description</b>
Strike Nefilim_053ec539	This strike sends a malware sample known as Nefilim. Nefilim ransomware shares much of its code with the popular RaaS known as Nemty, however, Nefilim instructs victims to contact the attackers via email rather than through a payment portal. Victims are mainly infected through vulnerable RDP services. Once the system has been infected, the malware establishes persistence and begins to exfiltrate credentials where possible. It will then deliver the ransomware payloads to the intended targets. The MD5 hash of this Nefilim sample is 053ec539c138afb99054bd362bb3ed71.
Strike Nefilim_0790a7e0	This strike sends a malware sample known as Nefilim. Nefilim ransomware shares much of its code with the popular RaaS known as Nemty, however, Nefilim instructs victims to contact the attackers via email rather than through a payment portal. Victims are mainly infected through vulnerable RDP services. Once the system has been infected, the malware establishes persistence and begins to exfiltrate credentials where possible. It will then deliver the ransomware payloads to the intended targets. The MD5 hash of this Nefilim sample is 0790a7e0a842e1de70de194054fa11b3.
Strike Nefilim_26c35850	This strike sends a malware sample known as Nefilim. Nefilim ransomware shares much of its code with the popular RaaS known as Nemty, however, Nefilim instructs victims to contact the attackers via email rather than through a payment portal. Victims are mainly infected through vulnerable RDP services. Once the system has been infected, the malware establishes persistence and begins to exfiltrate credentials where possible. It will then deliver the ransomware payloads to the intended targets. The MD5 hash of this Nefilim sample is 26c35850483c877ee23f476b38d58deb.
Strike Nefilim_3beb3d46	This strike sends a malware sample known as Nefilim. Nefilim ransomware shares much of its code with the popular RaaS known as Nemty, however, Nefilim instructs victims to contact the attackers via email rather than through a payment portal. Victims are mainly infected through vulnerable RDP services. Once the system has been infected, the malware establishes persistence and begins to exfiltrate credentials where possible. It will then deliver the ransomware payloads to the intended targets. The MD5 hash of this Nefilim sample is 3beb3d466bcc0977ec2dd66d72ab6bb3.
Strike Nefilim_5ff20e2b	This strike sends a malware sample known as Nefilim. Nefilim ransomware shares much of its code with the popular RaaS known as Nemty, however, Nefilim instructs victims to contact the attackers via email rather than through a payment portal. Victims are mainly infected through vulnerable RDP services. Once the system has been infected, the malware establishes persistence and begins to exfiltrate credentials where possible. It will then deliver the ransomware payloads to the intended targets. The MD5 hash of this Nefilim sample is 5ff20e2b723edb2d0fb27df4fc2c4468.
Strike Nefilim_659c4b68	This strike sends a malware sample known as Nefilim. Nefilim ransomware shares much of its code with the popular RaaS known as Nemty, however, Nefilim instructs victims to contact the attackers via email rather than through a payment portal. Victims are mainly infected through vulnerable RDP services. Once the system has been infected, the malware establishes persistence and begins to exfiltrate credentials where possible. It will then deliver the ransomware payloads to the intended targets. The MD5 hash of this Nefilim sample is 659c4b68f2027905def1af9249feeb3.

<b>Name</b>	<b>Description</b>
Strike Nefilim_70e4b9b7	This strike sends a malware sample known as Nefilim. Nefilim ransomware shares much of its code with the popular RaaS known as Nemty, however, Nefilim instructs victims to contact the attackers via email rather than through a payment portal. Victims are mainly infected through vulnerable RDP services. Once the system has been infected, the malware establishes persistence and begins to exfiltrate credentials where possible. It will then deliver the ransomware payloads to the intended targets. The MD5 hash of this Nefilim sample is 70e4b9b7a83473687e5784489d556c87.
Strike Nefilim_7354e71d	This strike sends a malware sample known as Nefilim. Nefilim ransomware shares much of its code with the popular RaaS known as Nemty, however, Nefilim instructs victims to contact the attackers via email rather than through a payment portal. Victims are mainly infected through vulnerable RDP services. Once the system has been infected, the malware establishes persistence and begins to exfiltrate credentials where possible. It will then deliver the ransomware payloads to the intended targets. The MD5 hash of this Nefilim sample is 7354e71d9c28e0c150cea3377e5f70d9.
Strike Nefilim_80cfda61	This strike sends a malware sample known as Nefilim. Nefilim ransomware shares much of its code with the popular RaaS known as Nemty, however, Nefilim instructs victims to contact the attackers via email rather than through a payment portal. Victims are mainly infected through vulnerable RDP services. Once the system has been infected, the malware establishes persistence and begins to exfiltrate credentials where possible. It will then deliver the ransomware payloads to the intended targets. The MD5 hash of this Nefilim sample is 80cfda61942eb4e71f286297a1158f48.
Strike Nefilim_8f90539c	This strike sends a malware sample known as Nefilim. Nefilim ransomware shares much of its code with the popular RaaS known as Nemty, however, Nefilim instructs victims to contact the attackers via email rather than through a payment portal. Victims are mainly infected through vulnerable RDP services. Once the system has been infected, the malware establishes persistence and begins to exfiltrate credentials where possible. It will then deliver the ransomware payloads to the intended targets. The MD5 hash of this Nefilim sample is 8f90539c405672016c0dec7ac3574eea.
Strike Nefilim_ce3cd1da	This strike sends a malware sample known as Nefilim. Nefilim ransomware shares much of its code with the popular RaaS known as Nemty, however, Nefilim instructs victims to contact the attackers via email rather than through a payment portal. Victims are mainly infected through vulnerable RDP services. Once the system has been infected, the malware establishes persistence and begins to exfiltrate credentials where possible. It will then deliver the ransomware payloads to the intended targets. The MD5 hash of this Nefilim sample is ce3cd1dab67814f5f153bccdaf502f4c.
Strike Nefilim_dc88265c	This strike sends a malware sample known as Nefilim. Nefilim ransomware shares much of its code with the popular RaaS known as Nemty, however, Nefilim instructs victims to contact the attackers via email rather than through a payment portal. Victims are mainly infected through vulnerable RDP services. Once the system has been infected, the malware establishes persistence and begins to exfiltrate credentials where possible. It will then deliver the ransomware payloads to the intended targets. The MD5 hash of this Nefilim sample is dc88265c361d73540a31c19583271fb0.

<b>Name</b>	<b>Description</b>
Strike Neflim_ddc50d4a	This strike sends a malware sample known as Neflim. Neflim ransomware shares much of its code with the popular RaaS known as Nemty, however, Neflim instructs victims to contact the attackers via email rather than through a payment portal. Victims are mainly infected through vulnerable RDP services. Once the system has been infected, the malware establishes persistence and begins to exfiltrate credentials where possible. It will then deliver the ransomware payloads to the intended targets. The MD5 hash of this Neflim sample is ddc50d4ae0674d854a845b3eb32508c3.
Strike Neflim_dfd4dbfd	This strike sends a malware sample known as Neflim. Neflim ransomware shares much of its code with the popular RaaS known as Nemty, however, Neflim instructs victims to contact the attackers via email rather than through a payment portal. Victims are mainly infected through vulnerable RDP services. Once the system has been infected, the malware establishes persistence and begins to exfiltrate credentials where possible. It will then deliver the ransomware payloads to the intended targets. The MD5 hash of this Neflim sample is dfd4dbfd7cbd6179fc371e5f887f189c.
Strike Nemty_0b33471b	This strike sends a malware sample known as Nemty. Nemty is a Ransomware-as-a-Service. Once obtained a user is granted access to a web portal where they are able to create custom versions of the ransomware. It has been spotted being delivered via email spam (malspam) campaigns, botnets, exploit kits, pay-pal dummy sites, and by brute-forcing RDP endpoints. The MD5 hash of this Nemty sample is 0b33471bbd9fb9f08983eff34ee4ddc9.
Strike Nemty_0e0b7b23	This strike sends a malware sample known as Nemty. Nemty is a Ransomware-as-a-Service. Once obtained a user is granted access to a web portal where they are able to create custom versions of the ransomware. It has been spotted being delivered via email spam (malspam) campaigns, botnets, exploit kits, pay-pal dummy sites, and by brute-forcing RDP endpoints. The MD5 hash of this Nemty sample is 0e0b7b238a06a2a37a4de06a5ab5e615.
Strike Nemty_0f3deda4	This strike sends a malware sample known as Nemty. Nemty is a Ransomware-as-a-Service. Once obtained a user is granted access to a web portal where they are able to create custom versions of the ransomware. It has been spotted being delivered via email spam (malspam) campaigns, botnets, exploit kits, pay-pal dummy sites, and by brute-forcing RDP endpoints. The MD5 hash of this Nemty sample is 0f3deda483df5e5f8043ea20297d243b.
Strike Nemty_348c3597	This strike sends a malware sample known as Nemty. Nemty is a Ransomware-as-a-Service. Once obtained a user is granted access to a web portal where they are able to create custom versions of the ransomware. It has been spotted being delivered via email spam (malspam) campaigns, botnets, exploit kits, pay-pal dummy sites, and by brute-forcing RDP endpoints. The MD5 hash of this Nemty sample is 348c3597c7d31c72ea723d5f7082ff87.
Strike Nemty_37aab6b	This strike sends a malware sample known as Nemty. Nemty is a Ransomware-as-a-Service. Once obtained a user is granted access to a web portal where they are able to create custom versions of the ransomware. It has been spotted being delivered via email spam (malspam) campaigns, botnets, exploit kits, pay-pal dummy sites, and by brute-forcing RDP endpoints. The MD5 hash of this Nemty sample is 37aab6b18c9c1b8150dae4f1d31e97d.

<b>Name</b>	<b>Description</b>
Strike Nemty_4ca39c0a	This strike sends a malware sample known as Nemty. Nemty is a Ransomware-as-a-Service. Once obtained a user is granted access to a web portal where they are able to create custom versions of the ransomware. It has been spotted being delivered via email spam (malspam) campaigns, botnets, exploit kits, pay-pal dummy sites, and by brute-forcing RDP endpoints. The MD5 hash of this Nemty sample is 4ca39c0aeb0daeb1be36173fa7c2a25e.
Strike Nemty_5126b883	This strike sends a malware sample known as Nemty. Nemty is a Ransomware-as-a-Service. Once obtained a user is granted access to a web portal where they are able to create custom versions of the ransomware. It has been spotted being delivered via email spam (malspam) campaigns, botnets, exploit kits, pay-pal dummy sites, and by brute-forcing RDP endpoints. The MD5 hash of this Nemty sample is 5126b88347c24245a9b141f76552064e.
Strike Nemty_5cc1bf61	This strike sends a malware sample known as Nemty. Nemty is a Ransomware-as-a-Service. Once obtained a user is granted access to a web portal where they are able to create custom versions of the ransomware. It has been spotted being delivered via email spam (malspam) campaigns, botnets, exploit kits, pay-pal dummy sites, and by brute-forcing RDP endpoints. The MD5 hash of this Nemty sample is 5cc1bf6122d38de907d558ec6851377c.
Strike Nemty_dcec4fed	This strike sends a malware sample known as Nemty. Nemty is a Ransomware-as-a-Service. Once obtained a user is granted access to a web portal where they are able to create custom versions of the ransomware. It has been spotted being delivered via email spam (malspam) campaigns, botnets, exploit kits, pay-pal dummy sites, and by brute-forcing RDP endpoints. The MD5 hash of this Nemty sample is dcec4fed3b60705eafdc5cbff4062375.
Strike Nemty_f2708056	This strike sends a malware sample known as Nemty. Nemty is a Ransomware-as-a-Service. Once obtained a user is granted access to a web portal where they are able to create custom versions of the ransomware. It has been spotted being delivered via email spam (malspam) campaigns, botnets, exploit kits, pay-pal dummy sites, and by brute-forcing RDP endpoints. The MD5 hash of this Nemty sample is f270805668e8aecf13d27c09055bad5d.
Strike NetWire_0c8f41a5	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is 0c8f41a5de36b16440634933d321f53b.
Strike NetWire_2564306c	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is 2564306c1854be464cf1ee8d502d239c.
Strike NetWire_28b9bf7d	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is 28b9bf7d0f9e9b59161ec62ff2575a72.
Strike NetWire_44a2821a	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is 44a2821a7450bbc974f00ccd35ad8b95.

<b>Name</b>	<b>Description</b>
Strike NetWire_44e152bf	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is 44e152bf429a978efaacc69aaa15f411.
Strike NetWire_4b68e3de	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is 4b68e3dee7caf6fc2d864033cb672361.
Strike NetWire_4ca8ed01	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is 4ca8ed01742bee59de7f772cc63485f6.
Strike NetWire_508b5cb0	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is 508b5cb051359afab99a9df733b6b9c7.
Strike NetWire_63f5b41a	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is 63f5b41acd46d5be96eb0da2799dd9cf.
Strike NetWire_6604862e	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is 6604862ee3afa04c9f4469173b4fb718.
Strike NetWire_6c7173b5	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is 6c7173b5cb3cc73798312015cca492b7.
Strike NetWire_886c6d07	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is 886c6d07ae020f48b3af4dd6357f558e.
Strike NetWire_91f0f2b9	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is 91f0f2b971edb3107925038ba495bc53.
Strike NetWire_9bd4363c	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is 9bd4363c63347e04ca78db9bbd577639.
Strike NetWire_a192512d	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is a192512d560035a6f5d02ec30e15c1f7.
Strike NetWire_a2256456	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is a2256456f1e328ba81bcabe984f24c86.

<b>Name</b>	<b>Description</b>
Strike NetWire_a482429d	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is a482429d1a13c6d0f3a879a6673391c5.
Strike NetWire_a71f9776	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is a71f9776f4e3339476cc98830697dd9a.
Strike NetWire_ab72b9d6	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is ab72b9d6a7017d9072cb33deb9d9d05d.
Strike NetWire_b1c25ebd	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is b1c25ebd733fcfa1c80420ddd3dad995.
Strike NetWire_b7cc74a4	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is b7cc74a4cc3ba9212fb38508cd65101d.
Strike NetWire_bbdec3e8	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is bbdec3e8962c07c7a23b54b56e44a9fb.
Strike NetWire_c687c676	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is c687c676f0cfa41262d69b051d600609.
Strike NetWire_c69a5fdc	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is c69a5fdc28d64c93f41e8944d88ebd1c.
Strike NetWire_c7ed1ef5	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is c7ed1ef5cb78c4fa7db734ea7bfc981b.
Strike NetWire_ca702192	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is ca702192cc583bfc559c418365a34521.
Strike NetWire_ca94e11b	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is ca94e11bf00bdf0bd4aa419b5d0e6ab1.
Strike NetWire_cdc526f8	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is cdc526f81bb9883a6027caf1befea29f.

<b>Name</b>	<b>Description</b>
Strike NetWire_d17967e7	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is d17967e7b8c68dc6cbc72201d2ceb6d2.
Strike NetWire_d245a5ba	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is d245a5ba7a237a97dc3464f7e1bddafc.
Strike NetWire_d5684dac	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is d5684dac5c8e7081056494a1b8c0eb3d.
Strike NetWire_e124339f	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is e124339f08506d6b5bab4d071784a65e.
Strike NetWire_edcc5bf8	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is edcc5bf8400b5967e585349e8372c017.
Strike NetWire_ee8b2b97	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is ee8b2b973977faff498e0ab45b01251c.
Strike NetWire_f05dad49	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is f05dad496a8b7f10a86804b48b60c009.
Strike NetWire_f6be0865	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is f6be08653b37cc6bf40b589ccc712b97.
Strike NetWire_fd06aeef	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is fd06aeefc7397dd23b37723a015bb4f7.
Strike NetWire_ffce5281	This strike sends a malware sample known as NetWire. Netwire is a Remote Access Trojan that lets attackers execute commands on the infected host. The MD5 hash of this NetWire sample is ffce5281717e13d43266ae5131d460a9.
Strike Netwalker_0537d845	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 0537d845ba099c6f2b708124eda13f1c.

<b>Name</b>	<b>Description</b>
Strike Netwalker_239163e6	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 239163e6019670e326087aa59adb5007.
Strike Netwalker_25c0fde0	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 25c0fde038e01fe84fd3df69c99e60a1.
Strike Netwalker_2f720c55	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 2f720c55dc1969da5299a45e031816ae.
Strike Netwalker_3cf36a7	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 3cf36a72db703e25aecd51eb74f0feb.
Strike Netwalker_4e59fba2	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 4e59fba21c5e9ec603f28a92d9efd8d0.
Strike Netwalker_59b00f60	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 59b00f607a7550af9a2332c730892845.
Strike Netwalker_5ce75526	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 5ce75526a25c81d0178d8092251013f0.
Strike Netwalker_5f55ac3d	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 5f55ac3dd18950583dadfffc1970745c5.
Strike Netwalker_608ac26e	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 608ac26ea80c189ed8e0f62dd4fd8ada.

<b>Name</b>	<b>Description</b>
Strike Netwalker_63eb7712	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 63eb7712d7c9d495e8a6be937bdb1960.
Strike Netwalker_645c720f	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 645c720ff0eb7d946ec3b4a6f609b7bc.
Strike Netwalker_6528c101	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 6528c1013ddb23f6eeeca08d02f3d7834.
Strike Netwalker_747dc998	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 747dc998c4cf60c6d40a77de18a9aa62.
Strike Netwalker_8fbc17d6	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 8fbc17d634009cb1ce261b5b3b2f2ecb.
Strike Netwalker_9172586c	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 9172586c2f870ab76eb0852d1f4dfaef.
Strike Netwalker_93f91bfc	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is 93f91bfcc1bf0c858fc7f3bd4536eba6.
Strike Netwalker_b49ea177	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is b49ea17739f484b2ccccf79f245186f3.
Strike Netwalker_bc758596	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is bc75859695f6c2c5ceda7e3be68e5d5a.

<b>Name</b>	<b>Description</b>
Strike Netwalker_cb78a77e	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is cb78a77e9ab26e4cf759e7d7b34bdbdc.
Strike Netwalker_cc113e42	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is cc113e42c52c6e4e7beca74829b89a68.
Strike Netwalker_d09cfda2	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is d09cfda29f178f57dbce6895cfb68372.
Strike Netwalker_dabbc5e5	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is dabbc5e50b9275cb2996c50fd81e64b4.
Strike Netwalker_f957f19c	This strike sends a malware sample known as Netwalker. Netwalker, also known as Mailto is Ransomware that encrypts Windows files on the compromised enterprise networks with the mailto extension. It uses the network of the victim to encrypt all Windows devices. The MD5 hash of this Netwalker sample is f957f19cd9d71abe3cb980ebe7f75d72.
Strike Nevada_b673d92b	This strike sends a malware sample known as Nevada. Nevada is ransomware written in Rust and is identified by the way in which it adds the .NEVADA extension to its encrypted files. This has the ability to delete itself, load hidden drives, encrypt shared folders, and run itself in safe mode. The MD5 hash of this Nevada sample is b673d92b77489d12779dc1fb5e8f6fdd.
Strike NineRAT_12e39941	This strike sends a malware sample known as NineRAT. NineRAT is a Remote Access Trojan (RAT) identified in the Lazarus Group's Operation Blacksmith campaign. It targets global enterprises, particularly those susceptible to n-day vulnerabilities like CVE-2021-44228, Lazarus focuses on industries such as manufacturing and security. NineRAT uses Telegram as a Command and Control (C2) channel, leveraging a legitimate service to avoid detection. The malware comprises a dropper, an instrumentor, and the RAT itself, demonstrating persistence through BAT scripts. The malware interacts with Telegram's API implemented using Dlang-based libraries for tasks such as authentication testing and file transfers. The MD5 hash of this NineRAT sample is 12e399411185e386c863954eaa6f6595.

<b>Name</b>	<b>Description</b>
Strike NineRAT_490bb2ab	<p>This strike sends a malware sample known as NineRAT. NineRAT is a Remote Access Trojan (RAT) identified in the Lazarus Group's Operation Blacksmith campaign. It targets global enterprises, particularly those susceptible to n-day vulnerabilities like CVE-2021-44228, Lazarus focuses on industries such as manufacturing and security. NineRAT uses Telegram as a Command and Control (C2) channel, leveraging a legitimate service to avoid detection. The malware comprises a dropper, an instrumentor, and the RAT itself, demonstrating persistence through BAT scripts. The malware interacts with Telegram's API implemented using Dlang-based libraries for tasks such as authentication testing and file transfers. The MD5 hash of this NineRAT sample is 490bb2abfdd5d4e185325c3a9fb9f5d7.</p>
Strike NineRAT_96d98c83	<p>This strike sends a malware sample known as NineRAT. NineRAT is a Remote Access Trojan (RAT) identified in the Lazarus Group's Operation Blacksmith campaign. It targets global enterprises, particularly those susceptible to n-day vulnerabilities like CVE-2021-44228, Lazarus focuses on industries such as manufacturing and security. NineRAT uses Telegram as a Command and Control (C2) channel, leveraging a legitimate service to avoid detection. The malware comprises a dropper, an instrumentor, and the RAT itself, demonstrating persistence through BAT scripts. The malware interacts with Telegram's API implemented using Dlang-based libraries for tasks such as authentication testing and file transfers. The MD5 hash of this NineRAT sample is 96d98c83daf368066efe3dd41a0dc622.</p>
Strike NineRAT_d13ac94a	<p>This strike sends a malware sample known as NineRAT. NineRAT is a Remote Access Trojan (RAT) identified in the Lazarus Group's Operation Blacksmith campaign. It targets global enterprises, particularly those susceptible to n-day vulnerabilities like CVE-2021-44228, Lazarus focuses on industries such as manufacturing and security. NineRAT uses Telegram as a Command and Control (C2) channel, leveraging a legitimate service to avoid detection. The malware comprises a dropper, an instrumentor, and the RAT itself, demonstrating persistence through BAT scripts. The malware interacts with Telegram's API implemented using Dlang-based libraries for tasks such as authentication testing and file transfers. The MD5 hash of this NineRAT sample is d13ac94aec9d82523b27d3c659e38d8a.</p>
Strike NineRAT_d9731b51	<p>This strike sends a malware sample known as NineRAT. NineRAT is a Remote Access Trojan (RAT) identified in the Lazarus Group's Operation Blacksmith campaign. It targets global enterprises, particularly those susceptible to n-day vulnerabilities like CVE-2021-44228, Lazarus focuses on industries such as manufacturing and security. NineRAT uses Telegram as a Command and Control (C2) channel, leveraging a legitimate service to avoid detection. The malware comprises a dropper, an instrumentor, and the RAT itself, demonstrating persistence through BAT scripts. The malware interacts with Telegram's API implemented using Dlang-based libraries for tasks such as authentication testing and file transfers. The MD5 hash of this NineRAT sample is d9731b51c936aa57207b0efe435ab056.</p>

<b>Name</b>	<b>Description</b>
Strike NineRAT_ea853503	This strike sends a malware sample known as NineRAT. NineRAT is a Remote Access Trojan (RAT) identified in the Lazarus Group's Operation Blacksmith campaign. It targets global enterprises, particularly those susceptible to n-day vulnerabilities like CVE-2021-44228, Lazarus focuses on industries such as manufacturing and security. NineRAT uses Telegram as a Command and Control (C2) channel, leveraging a legitimate service to avoid detection. The malware comprises a dropper, an instrumentor, and the RAT itself, demonstrating persistence through BAT scripts. The malware interacts with Telegram's API implemented using Dlang-based libraries for tasks such as authentication testing and file transfers. The MD5 hash of this NineRAT sample is ea853503ca1681e07de3e556604c4af7.
Strike Nood RAT_0a35e06f	This strike sends a malware sample known as Nood RAT. Nood RAT is a backdoor malware which is a Linux-compatible variant of Gh0st RAT. It enables threat actors to execute remote commands, manage files, and establish Socks proxies and port forwarding. It facilitates malicious activities such as downloading files, stealing internal files, executing commands, and serving as a proxy during lateral movement. The malware incorporates encryption to evade detection and operates based on commands received from the C&C server. The MD5 hash of this Nood RAT sample is 0a35e06f53c17ab1c8e18e7e0c0821d8.
Strike Nood RAT_35743db3	This strike sends a malware sample known as Nood RAT. Nood RAT is a backdoor malware which is a Linux-compatible variant of Gh0st RAT. It enables threat actors to execute remote commands, manage files, and establish Socks proxies and port forwarding. It facilitates malicious activities such as downloading files, stealing internal files, executing commands, and serving as a proxy during lateral movement. The malware incorporates encryption to evade detection and operates based on commands received from the C&C server. The MD5 hash of this Nood RAT sample is 35743db3dc333245ef5b69100721ced9.
Strike Nood RAT_4f3afdcf	This strike sends a malware sample known as Nood RAT. Nood RAT is a backdoor malware which is a Linux-compatible variant of Gh0st RAT. It enables threat actors to execute remote commands, manage files, and establish Socks proxies and port forwarding. It facilitates malicious activities such as downloading files, stealing internal files, executing commands, and serving as a proxy during lateral movement. The malware incorporates encryption to evade detection and operates based on commands received from the C&C server. The MD5 hash of this Nood RAT sample is 4f3afdcff8f7994b7d3d3fbbaa6858b4.
Strike Nood RAT_75838e5d	This strike sends a malware sample known as Nood RAT. Nood RAT is a backdoor malware which is a Linux-compatible variant of Gh0st RAT. It enables threat actors to execute remote commands, manage files, and establish Socks proxies and port forwarding. It facilitates malicious activities such as downloading files, stealing internal files, executing commands, and serving as a proxy during lateral movement. The malware incorporates encryption to evade detection and operates based on commands received from the C&C server. The MD5 hash of this Nood RAT sample is 75838e5d481da40db2e235a6d5a222ef.

<b>Name</b>	<b>Description</b>
Strike Nood RAT_7d631e5b	This strike sends a malware sample known as Nood RAT. Nood RAT is a backdoor malware which is a Linux-compatible variant of Gh0st RAT. It enables threat actors to execute remote commands, manage files, and establish Socks proxies and port forwarding. It facilitates malicious activities such as downloading files, stealing internal files, executing commands, and serving as a proxy during lateral movement. The malware incorporates encryption to evade detection and operates based on commands received from the C&C server. The MD5 hash of this Nood RAT sample is 7d631e5b0c78805dd5d440cce788d25b.
Strike Nood RAT_8457f71c	This strike sends a malware sample known as Nood RAT. Nood RAT is a backdoor malware which is a Linux-compatible variant of Gh0st RAT. It enables threat actors to execute remote commands, manage files, and establish Socks proxies and port forwarding. It facilitates malicious activities such as downloading files, stealing internal files, executing commands, and serving as a proxy during lateral movement. The malware incorporates encryption to evade detection and operates based on commands received from the C&C server. The MD5 hash of this Nood RAT sample is 8457f71c6a5fe83bb513d1dfba99271a.
Strike Nood RAT_905c2158	This strike sends a malware sample known as Nood RAT. Nood RAT is a backdoor malware which is a Linux-compatible variant of Gh0st RAT. It enables threat actors to execute remote commands, manage files, and establish Socks proxies and port forwarding. It facilitates malicious activities such as downloading files, stealing internal files, executing commands, and serving as a proxy during lateral movement. The malware incorporates encryption to evade detection and operates based on commands received from the C&C server. The MD5 hash of this Nood RAT sample is 905c2158fadfe31850766f010e149a0f.
Strike Nood RAT_97db3f76	This strike sends a malware sample known as Nood RAT. Nood RAT is a backdoor malware which is a Linux-compatible variant of Gh0st RAT. It enables threat actors to execute remote commands, manage files, and establish Socks proxies and port forwarding. It facilitates malicious activities such as downloading files, stealing internal files, executing commands, and serving as a proxy during lateral movement. The malware incorporates encryption to evade detection and operates based on commands received from the C&C server. The MD5 hash of this Nood RAT sample is 97db3f7676380f0baa3840ed5d5c1767.
Strike Nood RAT_a15ebd19	This strike sends a malware sample known as Nood RAT. Nood RAT is a backdoor malware which is a Linux-compatible variant of Gh0st RAT. It enables threat actors to execute remote commands, manage files, and establish Socks proxies and port forwarding. It facilitates malicious activities such as downloading files, stealing internal files, executing commands, and serving as a proxy during lateral movement. The malware incorporates encryption to evade detection and operates based on commands received from the C&C server. The MD5 hash of this Nood RAT sample is a15ebd19cac42b0297858018da62b1be.

<b>Name</b>	<b>Description</b>
Strike Nood RAT_b4910e99	This strike sends a malware sample known as Nood RAT. Nood RAT is a backdoor malware which is a Linux-compatible variant of Gh0st RAT. It enables threat actors to execute remote commands, manage files, and establish Socks proxies and port forwarding. It facilitates malicious activities such as downloading files, stealing internal files, executing commands, and serving as a proxy during lateral movement. The malware incorporates encryption to evade detection and operates based on commands received from the C&C server. The MD5 hash of this Nood RAT sample is b4910e998cf58da452f8151b71c868cb.
Strike Nood RAT_c440bd81	This strike sends a malware sample known as Nood RAT. Nood RAT is a backdoor malware which is a Linux-compatible variant of Gh0st RAT. It enables threat actors to execute remote commands, manage files, and establish Socks proxies and port forwarding. It facilitates malicious activities such as downloading files, stealing internal files, executing commands, and serving as a proxy during lateral movement. The malware incorporates encryption to evade detection and operates based on commands received from the C&C server. The MD5 hash of this Nood RAT sample is c440bd814be37fac669567131c4ba996.
Strike Nood RAT_d9f00f71	This strike sends a malware sample known as Nood RAT. Nood RAT is a backdoor malware which is a Linux-compatible variant of Gh0st RAT. It enables threat actors to execute remote commands, manage files, and establish Socks proxies and port forwarding. It facilitates malicious activities such as downloading files, stealing internal files, executing commands, and serving as a proxy during lateral movement. The malware incorporates encryption to evade detection and operates based on commands received from the C&C server. The MD5 hash of this Nood RAT sample is d9f00f71efabdfcca7c63d4b0805673c.
Strike Noon_1e30ab4c	This strike sends a polymorphic malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The binary has been packed using upx packer, with the default options. The MD5 hash of this Noon sample is 1e30ab4cdfe0dd94844d6c98421747d4.
Strike Noon_2874228a	This strike sends a malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The MD5 hash of this Noon sample is 2874228a62abe22aa666e86fde09ab32.
Strike Noon_2e86611a	This strike sends a polymorphic malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Noon sample is 2e86611af6e0724df48c91b5e4da4c7f.
Strike Noon_3bacdeae	This strike sends a polymorphic malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Noon sample is 3bacdeae83ff868acb771dfbaeae1.

<b>Name</b>	<b>Description</b>
Strike Noon_4f67bb15	This strike sends a polymorphic malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Noon sample is 4f67bb159e04ca79e524bf27b4786999.
Strike Noon_6ab1cb55	This strike sends a malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The MD5 hash of this Noon sample is 6ab1cb55076059871d68ebd5504b28b3.
Strike Noon_82eae68b	This strike sends a malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The MD5 hash of this Noon sample is 82eae68b59dd0160dab6531cb4a33190.
Strike Noon_8c8f0ecd	This strike sends a malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The MD5 hash of this Noon sample is 8c8f0ecdc72cc10548bc34282dca3131.
Strike Noon_8d377ac9	This strike sends a malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The MD5 hash of this Noon sample is 8d377ac907cbb773d6a7065397c5248c.
Strike Noon_9beb8ed7	This strike sends a malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The MD5 hash of this Noon sample is 9beb8ed71c0c19c8172511b0f54db154.
Strike Noon_af6c6478	This strike sends a malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The MD5 hash of this Noon sample is af6c647815066e4fe89f71a761e0219c.
Strike Noon_b1f1ad58	This strike sends a polymorphic malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The binary has been packed using upx packer, with the default options. The MD5 hash of this Noon sample is b1f1ad58fab8c4f1e61c7a27ff40e970.

<b>Name</b>	<b>Description</b>
Strike Noon_bb90be3c	This strike sends a malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The MD5 hash of this Noon sample is bb90be3c58d26db5800b87cc6e3c79f5.
Strike Noon_c2193a36	This strike sends a malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The MD5 hash of this Noon sample is c2193a3639998662a87d53d77295edae.
Strike Noon_c95289ac	This strike sends a polymorphic malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The binary has random bytes appended at the end of the file. The MD5 hash of this Noon sample is c95289ac71d9a39056073a533ac87c9e.
Strike Noon_d16f93d2	This strike sends a polymorphic malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The binary has random bytes appended at the end of the file. The MD5 hash of this Noon sample is d16f93d2d6b85ee93bae643c08367058.
Strike Noon_e6de7580	This strike sends a malware sample known as Noon. Noon malware can execute other malware binaries. Once deployed it will connect to remote servers and push sensitive information to the attackers. This malware also maintains persistence on the victim machines. The MD5 hash of this Noon sample is e6de7580d7646c8b3f2cfb317734512a.
Strike Ntopsy_4a7ed329	This strike sends a malware sample known as Ntopsy. Ntopsy is a malware categorized as a Network Provider DLL module, strategically designed for the theft of user credentials. This malicious tool is adept at establishing backdoor capabilities, enabling command and control (C2), and exfiltrating sensitive information. To execute credential theft, the threat actor deploys a custom DLL module functioning as a Network Provider. Through the manipulation of the authentication process, Ntopsy gains access to user credentials whenever authentication attempts are made. The MD5 hash of this Ntopsy sample is 4a7ed329d2fc81b2561e520edaa5dc2b.
Strike Ntopsy_626adb5f	This strike sends a malware sample known as Ntopsy. Ntopsy is a malware categorized as a Network Provider DLL module, strategically designed for the theft of user credentials. This malicious tool is adept at establishing backdoor capabilities, enabling command and control (C2), and exfiltrating sensitive information. To execute credential theft, the threat actor deploys a custom DLL module functioning as a Network Provider. Through the manipulation of the authentication process, Ntopsy gains access to user credentials whenever authentication attempts are made. The MD5 hash of this Ntopsy sample is 626adb5fa6ee8a718e1dc7d5397e56ca.

Name	Description
Strike Ntopsy_78e4855a	This strike sends a malware sample known as Ntopsy. Ntopsy is a malware categorized as a Network Provider DLL module, strategically designed for the theft of user credentials. This malicious tool is adept at establishing backdoor capabilities, enabling command and control (C2), and exfiltrating sensitive information. To execute credential theft, the threat actor deploys a custom DLL module functioning as a Network Provider. Through the manipulation of the authentication process, Ntopsy gains access to user credentials whenever authentication attempts are made. The MD5 hash of this Ntopsy sample is 78e4855a26ce139ad6e27e3233b855c2.
Strike Ntopsy_c49d5658	This strike sends a malware sample known as Ntopsy. Ntopsy is a malware categorized as a Network Provider DLL module, strategically designed for the theft of user credentials. This malicious tool is adept at establishing backdoor capabilities, enabling command and control (C2), and exfiltrating sensitive information. To execute credential theft, the threat actor deploys a custom DLL module functioning as a Network Provider. Through the manipulation of the authentication process, Ntopsy gains access to user credentials whenever authentication attempts are made. The MD5 hash of this Ntopsy sample is c49d5658f785b2cc9608755d5ace2add.
Strike Ntopsy_dfe57386	This strike sends a malware sample known as Ntopsy. Ntopsy is a malware categorized as a Network Provider DLL module, strategically designed for the theft of user credentials. This malicious tool is adept at establishing backdoor capabilities, enabling command and control (C2), and exfiltrating sensitive information. To execute credential theft, the threat actor deploys a custom DLL module functioning as a Network Provider. Through the manipulation of the authentication process, Ntopsy gains access to user credentials whenever authentication attempts are made. The MD5 hash of this Ntopsy sample is dfe573867aff9267fc8d7926c5a8454e.
Strike Ntopsy_fd37b309	This strike sends a malware sample known as Ntopsy. Ntopsy is a malware categorized as a Network Provider DLL module, strategically designed for the theft of user credentials. This malicious tool is adept at establishing backdoor capabilities, enabling command and control (C2), and exfiltrating sensitive information. To execute credential theft, the threat actor deploys a custom DLL module functioning as a Network Provider. Through the manipulation of the authentication process, Ntopsy gains access to user credentials whenever authentication attempts are made. The MD5 hash of this Ntopsy sample is fd37b309870f9fb200232b1051431831.
Strike ONNX Store_0250a5ba	This strike sends a malware sample known as ONNX Store. ONNX Store is a PhaaS or Phishing-as-a-Platform malware. The attack resembles an original Microsoft 365 login page that will tricks users into entering their authentication credentials. This new PhaaS ONNX has the ability to control their operations via Telegram bots and support is provided by a support channel. The MD5 hash of this ONNX Store sample is 0250a5ba26791e7ffddb4b294d486479.
Strike ONNX Store_10d6e16a	This strike sends a malware sample known as ONNX Store. ONNX Store is a PhaaS or Phishing-as-a-Platform malware. The attack resembles an original Microsoft 365 login page that will tricks users into entering their authentication credentials. This new PhaaS ONNX has the ability to control their operations via Telegram bots and support is provided by a support channel. The MD5 hash of this ONNX Store sample is 10d6e16a05965be5bc0059131dc5ae7c.

<b>Name</b>	<b>Description</b>
Strike ONNX Store_15ef89d1	This strike sends a malware sample known as ONNX Store. ONNX Store is a PhaaS or Phishing-as-a-Platform malware. The attack resembles an original Microsoft 365 login page that will tricks users into entering their authentication credentials. This new PhaaS ONNX has the ability to control their operations via Telegram bots and support is provided by a support channel. The MD5 hash of this ONNX Store sample is 15ef89d1a2aa023ab664e1adcd75cbfd.
Strike ONNX Store_1932d823	This strike sends a malware sample known as ONNX Store. ONNX Store is a PhaaS or Phishing-as-a-Platform malware. The attack resembles an original Microsoft 365 login page that will tricks users into entering their authentication credentials. This new PhaaS ONNX has the ability to control their operations via Telegram bots and support is provided by a support channel. The MD5 hash of this ONNX Store sample is 1932d8238769b203693d1bbb56e541d2.
Strike ONNX Store_2a0576dc	This strike sends a malware sample known as ONNX Store. ONNX Store is a PhaaS or Phishing-as-a-Platform malware. The attack resembles an original Microsoft 365 login page that will tricks users into entering their authentication credentials. This new PhaaS ONNX has the ability to control their operations via Telegram bots and support is provided by a support channel. The MD5 hash of this ONNX Store sample is 2a0576dc8628b3f27190755d291750e4.
Strike ONNX Store_3f042b12	This strike sends a malware sample known as ONNX Store. ONNX Store is a PhaaS or Phishing-as-a-Platform malware. The attack resembles an original Microsoft 365 login page that will tricks users into entering their authentication credentials. This new PhaaS ONNX has the ability to control their operations via Telegram bots and support is provided by a support channel. The MD5 hash of this ONNX Store sample is 3f042b126e54b3a57485bf034d31fb39.
Strike ONNX Store_6193c137	This strike sends a malware sample known as ONNX Store. ONNX Store is a PhaaS or Phishing-as-a-Platform malware. The attack resembles an original Microsoft 365 login page that will tricks users into entering their authentication credentials. This new PhaaS ONNX has the ability to control their operations via Telegram bots and support is provided by a support channel. The MD5 hash of this ONNX Store sample is 6193c137f3b5b0da106b86f74670cf6f.
Strike ONNX Store_69804443	This strike sends a malware sample known as ONNX Store. ONNX Store is a PhaaS or Phishing-as-a-Platform malware. The attack resembles an original Microsoft 365 login page that will tricks users into entering their authentication credentials. This new PhaaS ONNX has the ability to control their operations via Telegram bots and support is provided by a support channel. The MD5 hash of this ONNX Store sample is 6980444399f1de17eec169e844d0b30e.
Strike ONNX Store_83dac377	This strike sends a malware sample known as ONNX Store. ONNX Store is a PhaaS or Phishing-as-a-Platform malware. The attack resembles an original Microsoft 365 login page that will tricks users into entering their authentication credentials. This new PhaaS ONNX has the ability to control their operations via Telegram bots and support is provided by a support channel. The MD5 hash of this ONNX Store sample is 83dac37771e8592e006f671666ebf590.
Strike ONNX Store_d125e7ed	This strike sends a malware sample known as ONNX Store. ONNX Store is a PhaaS or Phishing-as-a-Platform malware. The attack resembles an original Microsoft 365 login page that will tricks users into entering their authentication credentials. This new PhaaS ONNX has the ability to control their operations via Telegram bots and support is provided by a support channel. The MD5 hash of this ONNX Store sample is d125e7ed32bc2ce320489f5b5cd3ffdc.

Name	Description
Strike OneClik_0689b3ce	This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is 0689b3ce6ace42d324a70c8dc3bf1b85.
Strike OneClik_129399b8	This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is 129399b838d6526751faf16ecea92942.
Strike OneClik_22850f5d	This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is 22850f5d9467812c648996db617af3d7.
Strike OneClik_2afcc359	This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is 2afcc359528893cc2649957c82200937.
Strike OneClik_2cbdd117	This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is 2cbdd1172f31ab41f1590d9499da8dcb.

<b>Name</b>	<b>Description</b>
Strike OneClik_33b2bfe7	<p>This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is 33b2bfe7bd62c0ee00601083995729fb.</p>
Strike OneClik_6ed1b057	<p>This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is 6ed1b057283d825427f1b8436ffa9697.</p>
Strike OneClik_6fd88ca0	<p>This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is 6fd88ca06bfc56e588af2afc27510272.</p>
Strike OneClik_7151915a	<p>This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is 7151915acf75874f68d9b6ab9b8ced2c.</p>
Strike OneClik_7a4fbcd17	<p>This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is 7a4fbcd177c0967d43ec25691c8eadfc4.</p>

<b>Name</b>	<b>Description</b>
Strike OneClik_82687992	<p>This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is 82687992c82fdbd2c95ea5b77f21dcb28.</p>
Strike OneClik_844e461b	<p>This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is 844e461bdcb9ffc0264efc2b9e1ff1b2.</p>
Strike OneClik_9516e498	<p>This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is 9516e49889350bba029b9c224e26338f.</p>
Strike OneClik_992d0468	<p>This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is 992d0468082174925602858b426b7603.</p>
Strike OneClik_af3787af	<p>This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is af3787af042c1a83153cbc83630aff0f.</p>

Name	Description
Strike OneClik_c75fc34d	This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is c75fc34d3fef4c42f36fd940805ccaaef.
Strike OneClik_cfac7982	This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is cfac7982a53d70872f4ac7155e5e3581.
Strike OneClik_e355e138	This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is e355e138bd2e5179c75f1e382e8bbb05.
Strike OneClik_ffdc83bb	This strike sends a malware sample known as OneClik. This strike sends a malware sample known as OneClik RunnerBeacon. OneClik is a ClickOnce-based loader that delivers RunnerBeacon, a Golang backdoor used in red team campaigns targeting energy infrastructure. It abuses ClickOnce manifests hosted on Azure to launch dfsvc.exe, which is hijacked using AppDomainManager injection to load a .NET loader. RunnerBeacon executes in memory, uses RC4-encrypted MessagePack for C2 over AWS services like CloudFront and API Gateway, and performs shell commands, file operations, port scanning, and tunneling, while evading detection through anti-analysis checks. The MD5 hash of this OneClik sample is ffdc83bb65b97ef41b7d5f18543c573f.
Strike Onyx Sleet Proxy_19a05a55	This strike sends a malware sample known as Onyx Sleet Proxy. Onyx Sleet Proxy Tool, this proxy tool loader is malware that has been associated with the Onyx Sleet North Korean cyber attacks that follow successful exploitation of a TeamCity Service. The malware is a payload responsible for setting up a persistent connection between the compromised host and a remote C2 server. The MD5 hash of this Onyx Sleet Proxy sample is 19a05a559b0c478f3049cd414300a340.

Name	Description
Strike Operation Digital Eye_00a928b6	This strike sends a malware sample known as Operation Digital Eye. Operation Digital Eye is a cyberespionage attack campaign that took place in the summer months of 2024. The exact threat actors associated with the attack are unknown but it is currently being linked to several Chinese APT groups. Initial access was obtained via SQL injection vulnerabilities, and to establish the attackers used a PHP webshell. The malware used in the campaign allowed for credential exfiltration via dumping the LSASS memory and SAM database. They then moved laterally across the network with RDP and pass-the-hash techniques utilizing a custom Mimikatz executable. Finally the attackers used a custom digitally signed version of Visual Studio Code run with winsw to allow the binary to run as a service to create a tunnel for the attackers to communicate with. This malware is one of the binaries used in this attack campaign. The MD5 hash of this Operation Digital Eye sample is 00a928b681e545c0ae859c56f2dfd160.
Strike Operation Digital Eye_01c926d6	This strike sends a malware sample known as Operation Digital Eye. Operation Digital Eye is a cyberespionage attack campaign that took place in the summer months of 2024. The exact threat actors associated with the attack are unknown but it is currently being linked to several Chinese APT groups. Initial access was obtained via SQL injection vulnerabilities, and to establish the attackers used a PHP webshell. The malware used in the campaign allowed for credential exfiltration via dumping the LSASS memory and SAM database. They then moved laterally across the network with RDP and pass-the-hash techniques utilizing a custom Mimikatz executable. Finally the attackers used a custom digitally signed version of Visual Studio Code run with winsw to allow the binary to run as a service to create a tunnel for the attackers to communicate with. This malware is one of the binaries used in this attack campaign. The MD5 hash of this Operation Digital Eye sample is 01c926d62f2cf5c61bd477a2edef1d13.
Strike Operation Digital Eye_0f4da440	This strike sends a malware sample known as Operation Digital Eye. Operation Digital Eye is a cyberespionage attack campaign that took place in the summer months of 2024. The exact threat actors associated with the attack are unknown but it is currently being linked to several Chinese APT groups. Initial access was obtained via SQL injection vulnerabilities, and to establish the attackers used a PHP webshell. The malware used in the campaign allowed for credential exfiltration via dumping the LSASS memory and SAM database. They then moved laterally across the network with RDP and pass-the-hash techniques utilizing a custom Mimikatz executable. Finally the attackers used a custom digitally signed version of Visual Studio Code run with winsw to allow the binary to run as a service to create a tunnel for the attackers to communicate with. This malware is one of the binaries used in this attack campaign. The MD5 hash of this Operation Digital Eye sample is 0f4da44035f13084a3af5746175dd983.

<b>Name</b>	<b>Description</b>
Strike Operation Digital Eye_23db5c18	<p>This strike sends a malware sample known as Operation Digital Eye. Operation Digital Eye is a cyberespionage attack campaign that took place in the summer months of 2024. The exact threat actors associated with the attack are unknown but it is currently being linked to several Chinese APT groups. Initial access was obtained via SQL injection vulnerabilities, and to establish the attackers used a PHP webshell. The malware used in the campaign allowed for credential exfiltration via dumping the LSASS memory and SAM database. They then moved laterally across the network with RDP and pass-the-hash techniques utilizing a custom Mimikatz executable. Finally the attackers used a custom digitally signed version of Visual Studio Code run with winsw to allow the binary to run as a service to create a tunnel for the attackers to communicate with. This malware is one of the binaries used in this attack campaign. The MD5 hash of this Operation Digital Eye sample is 23db5c18fa1873334eb9ead3c1707cf.</p>
Strike Operation Digital Eye_6f21f284	<p>This strike sends a malware sample known as Operation Digital Eye. Operation Digital Eye is a cyberespionage attack campaign that took place in the summer months of 2024. The exact threat actors associated with the attack are unknown but it is currently being linked to several Chinese APT groups. Initial access was obtained via SQL injection vulnerabilities, and to establish the attackers used a PHP webshell. The malware used in the campaign allowed for credential exfiltration via dumping the LSASS memory and SAM database. They then moved laterally across the network with RDP and pass-the-hash techniques utilizing a custom Mimikatz executable. Finally the attackers used a custom digitally signed version of Visual Studio Code run with winsw to allow the binary to run as a service to create a tunnel for the attackers to communicate with. This malware is one of the binaries used in this attack campaign. The MD5 hash of this Operation Digital Eye sample is 6f21f284776f3766938f197117674606.</p>
Strike Operation Digital Eye_7972cacd	<p>This strike sends a malware sample known as Operation Digital Eye. Operation Digital Eye is a cyberespionage attack campaign that took place in the summer months of 2024. The exact threat actors associated with the attack are unknown but it is currently being linked to several Chinese APT groups. Initial access was obtained via SQL injection vulnerabilities, and to establish the attackers used a PHP webshell. The malware used in the campaign allowed for credential exfiltration via dumping the LSASS memory and SAM database. They then moved laterally across the network with RDP and pass-the-hash techniques utilizing a custom Mimikatz executable. Finally the attackers used a custom digitally signed version of Visual Studio Code run with winsw to allow the binary to run as a service to create a tunnel for the attackers to communicate with. This malware is one of the binaries used in this attack campaign. The MD5 hash of this Operation Digital Eye sample is 7972cacd0c56967745b152896dd7baa1.</p>

Name	Description
Strike Operation Digital Eye_7b3d35f5	This strike sends a malware sample known as Operation Digital Eye. Operation Digital Eye is a cyberespionage attack campaign that took place in the summer months of 2024. The exact threat actors associated with the attack are unknown but it is currently being linked to several Chinese APT groups. Initial access was obtained via SQL injection vulnerabilities, and to establish the attackers used a PHP webshell. The malware used in the campaign allowed for credential exfiltration via dumping the LSASS memory and SAM database. They then moved laterally across the network with RDP and pass-the-hash techniques utilizing a custom Mimikatz executable. Finally the attackers used a custom digitally signed version of Visual Studio Code run with winsw to allow the binary to run as a service to create a tunnel for the attackers to communicate with. This malware is one of the binaries used in this attack campaign. The MD5 hash of this Operation Digital Eye sample is 7b3d35f554c2f56e0ff0a41b4483f40f.
Strike Operation Digital Eye_88a40420	This strike sends a malware sample known as Operation Digital Eye. Operation Digital Eye is a cyberespionage attack campaign that took place in the summer months of 2024. The exact threat actors associated with the attack are unknown but it is currently being linked to several Chinese APT groups. Initial access was obtained via SQL injection vulnerabilities, and to establish the attackers used a PHP webshell. The malware used in the campaign allowed for credential exfiltration via dumping the LSASS memory and SAM database. They then moved laterally across the network with RDP and pass-the-hash techniques utilizing a custom Mimikatz executable. Finally the attackers used a custom digitally signed version of Visual Studio Code run with winsw to allow the binary to run as a service to create a tunnel for the attackers to communicate with. This malware is one of the binaries used in this attack campaign. The MD5 hash of this Operation Digital Eye sample is 88a404201bad69548783a745c0aece2b.
Strike Operation Digital Eye_937ec6c9	This strike sends a malware sample known as Operation Digital Eye. Operation Digital Eye is a cyberespionage attack campaign that took place in the summer months of 2024. The exact threat actors associated with the attack are unknown but it is currently being linked to several Chinese APT groups. Initial access was obtained via SQL injection vulnerabilities, and to establish the attackers used a PHP webshell. The malware used in the campaign allowed for credential exfiltration via dumping the LSASS memory and SAM database. They then moved laterally across the network with RDP and pass-the-hash techniques utilizing a custom Mimikatz executable. Finally the attackers used a custom digitally signed version of Visual Studio Code run with winsw to allow the binary to run as a service to create a tunnel for the attackers to communicate with. This malware is one of the binaries used in this attack campaign. The MD5 hash of this Operation Digital Eye sample is 937ec6c95c5469081e2f21506e5ee8f4.

Name	Description
Strike Operation Digital Eye_987a5fb6	<p>This strike sends a malware sample known as Operation Digital Eye. Operation Digital Eye is a cyberespionage attack campaign that took place in the summer months of 2024. The exact threat actors associated with the attack are unknown but it is currently being linked to several Chinese APT groups. Initial access was obtained via SQL injection vulnerabilities, and to establish the attackers used a PHP webshell. The malware used in the campaign allowed for credential exfiltration via dumping the LSASS memory and SAM database. They then moved laterally across the network with RDP and pass-the-hash techniques utilizing a custom Mimikatz executable. Finally the attackers used a custom digitally signed version of Visual Studio Code run with winsw to allow the binary to run as a service to create a tunnel for the attackers to communicate with. This malware is one of the binaries used in this attack campaign. The MD5 hash of this Operation Digital Eye sample is 987a5fb6e281db083e26619b74057be0.</p>
Strike Operation Digital Eye_a2cf1e86	<p>This strike sends a malware sample known as Operation Digital Eye. Operation Digital Eye is a cyberespionage attack campaign that took place in the summer months of 2024. The exact threat actors associated with the attack are unknown but it is currently being linked to several Chinese APT groups. Initial access was obtained via SQL injection vulnerabilities, and to establish the attackers used a PHP webshell. The malware used in the campaign allowed for credential exfiltration via dumping the LSASS memory and SAM database. They then moved laterally across the network with RDP and pass-the-hash techniques utilizing a custom Mimikatz executable. Finally the attackers used a custom digitally signed version of Visual Studio Code run with winsw to allow the binary to run as a service to create a tunnel for the attackers to communicate with. This malware is one of the binaries used in this attack campaign. The MD5 hash of this Operation Digital Eye sample is a2cf1e86c993d23a51022fc7784a84eb.</p>
Strike Operation Digital Eye_e08998c2	<p>This strike sends a malware sample known as Operation Digital Eye. Operation Digital Eye is a cyberespionage attack campaign that took place in the summer months of 2024. The exact threat actors associated with the attack are unknown but it is currently being linked to several Chinese APT groups. Initial access was obtained via SQL injection vulnerabilities, and to establish the attackers used a PHP webshell. The malware used in the campaign allowed for credential exfiltration via dumping the LSASS memory and SAM database. They then moved laterally across the network with RDP and pass-the-hash techniques utilizing a custom Mimikatz executable. Finally the attackers used a custom digitally signed version of Visual Studio Code run with winsw to allow the binary to run as a service to create a tunnel for the attackers to communicate with. This malware is one of the binaries used in this attack campaign. The MD5 hash of this Operation Digital Eye sample is e08998c219260a4b55776c46f942d854.</p>

<b>Name</b>	<b>Description</b>
Strike Operation Digital Eye_ef3f4101	This strike sends a malware sample known as Operation Digital Eye. Operation Digital Eye is a cyberespionage attack campaign that took place in the summer months of 2024. The exact threat actors associated with the attack are unknown but it is currently being linked to several Chinese APT groups. Initial access was obtained via SQL injection vulnerabilities, and to establish the attackers used a PHP webshell. The malware used in the campaign allowed for credential exfiltration via dumping the LSASS memory and SAM database. They then moved laterally across the network with RDP and pass-the-hash techniques utilizing a custom Mimikatz executable. Finally the attackers used a custom digitally signed version of Visual Studio Code run with winsw to allow the binary to run as a service to create a tunnel for the attackers to communicate with. This malware is one of the binaries used in this attack campaign. The MD5 hash of this Operation Digital Eye sample is ef3f4101ebab9ee934cd8c9e5e2b2923.
Strike Operation Digital Eye_fb58bd95	This strike sends a malware sample known as Operation Digital Eye. Operation Digital Eye is a cyberespionage attack campaign that took place in the summer months of 2024. The exact threat actors associated with the attack are unknown but it is currently being linked to several Chinese APT groups. Initial access was obtained via SQL injection vulnerabilities, and to establish the attackers used a PHP webshell. The malware used in the campaign allowed for credential exfiltration via dumping the LSASS memory and SAM database. They then moved laterally across the network with RDP and pass-the-hash techniques utilizing a custom Mimikatz executable. Finally the attackers used a custom digitally signed version of Visual Studio Code run with winsw to allow the binary to run as a service to create a tunnel for the attackers to communicate with. This malware is one of the binaries used in this attack campaign. The MD5 hash of this Operation Digital Eye sample is fb58bd95869f7e7554ffecff6809b508.
Strike Parite_01283cb5	This strike sends a polymorphic malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Parite sample is 01283cb5e169eaf9469babce95813512.
Strike Parite_15bd6120	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 15bd612023dd9b0ac62bdee6e7bba66e.
Strike Parite_1c38a261	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 1c38a2612991c580164bde56e3eb8504.
Strike Parite_2b034e31	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 2b034e31d39c0b5da9cc1db6834286e3.

<b>Name</b>	<b>Description</b>
Strike Parite_2e2e8301	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 2e2e8301ffa3bb44d35bfb752287960b.
Strike Parite_2ec058f2	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 2ec058f2b61c54c9341ce3df7c656aa3.
Strike Parite_4a7f3101	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 4a7f3101b1b4c84bfe166e674b569327.
Strike Parite_5add5f72	This strike sends a polymorphic malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Parite sample is 5add5f7297dae55218258dca3e93ec86.
Strike Parite_5af55b8b	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 5af55b8b4baad60536f72a56dec47833.
Strike Parite_793240d6	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 793240d66e7c9e985122d22ed9789649.
Strike Parite_7d0bdb44	This strike sends a polymorphic malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The binary has random bytes appended at the end of the file. The MD5 hash of this Parite sample is 7d0bdb44911b674b383d2453348c5198.
Strike Parite_84d6794b	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 84d6794b910f1ffbdd0384e0c032b34c.
Strike Parite_89c48076	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 89c480763a7b1f948a6a6c7a8b505ff0.
Strike Parite_8d88b34a	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 8d88b34a520bd2c7facfb0a6f46a531c.

<b>Name</b>	<b>Description</b>
Strike Parite_8efafc0e	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 8efafc0e3bad22d31f1c947c9e030e02.
Strike Parite_90ccb11	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 90ccb110fa607e39135fd048fd39590.
Strike Parite_99930ff7	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 99930ff7c02e7869c75364b632829a9f.
Strike Parite_9d0e9141	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is 9d0e914114bc9a7aa22391fea77550ac.
Strike Parite_a189ce7a	This strike sends a polymorphic malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Parite sample is a189ce7a80f28ebc564eae71beb3d1c8.
Strike Parite_a275b15b	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is a275b15b1bf7e1cee0b9724e6540d08c.
Strike Parite_a88566b7	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is a88566b7cac7895c5a2495213778061e.
Strike Parite_b49a537c	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is b49a537c826bccbe33b849f2123ecf3d.
Strike Parite_b6c9ca37	This strike sends a polymorphic malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The binary has the checksum removed in the PE file format. The MD5 hash of this Parite sample is b6c9ca37f26c6798814bb4ad18725c6a.
Strike Parite_ba15c6e3	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is ba15c6e34c7bb981b450db5833dd3d45.

<b>Name</b>	<b>Description</b>
Strike Parite_c1f0c0b7	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is c1f0c0b7a75e3b39d592fdb76bb49fc4.
Strike Parite_c29f4e0b	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is c29f4e0b3381fd84965a3e43c11db687.
Strike Parite_c3534d0b	This strike sends a polymorphic malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Parite sample is c3534d0b88e6c899fcefcf418822c70.
Strike Parite_ccca7711	This strike sends a polymorphic malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Parite sample is ccca7711eef4f0efe4af6af0e7083788.
Strike Parite_cd97f5f6	This strike sends a polymorphic malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The binary has the checksum removed in the PE file format. The MD5 hash of this Parite sample is cd97f5f6f33db7b85479ecf96d9b121d.
Strike Parite_d0d4548b	This strike sends a polymorphic malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The binary has random bytes appended at the end of the file. The MD5 hash of this Parite sample is d0d4548b97635ea9057800b570ca61ca.
Strike Parite_d7598adb	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is d7598adb41892c2e937aeb768915ab09.
Strike Parite_e40cc4c0	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is e40cc4c015e1440dc91509e35e5f2c62.
Strike Parite_f3fe002a	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victims local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is f3fe002a74ed38ec3589d3cd447bf853.

<b>Name</b>	<b>Description</b>
Strike Parite_f5a59242	This strike sends a polymorphic malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victim's local machine and then spreads throughout the targeted network. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Parite sample is f5a59242439ca4b24375e60b14636f31.
Strike Parite_fa61b650	This strike sends a malware sample known as Parite. Parite is a polymorphic file infector. This malware begins by infecting executables on a victim's local machine and then spreads throughout the targeted network. The MD5 hash of this Parite sample is fa61b6509603208bbafbc0bf49e9ad9d.
Strike Pegasus_7c3ad8fe	This strike sends an Android malware sample known as Pegasus. It is a spyware developed by the NSO group which exfiltrates data from installed social media apps, steals stored credentials, takes screenshots, photos and many more malicious activities. The MD5 hash of this Pegasus sample is 7c3ad8fec33465fed6563bbfabb5b13d.
Strike Pegasus_8468af0e	This strike sends an Android malware sample known as Pegasus. It is a spyware developed by the NSO group which exfiltrates data from installed social media apps, steals stored credentials, takes screenshots, photos and many more malicious activities. NOTE: The APK samples have been signed with custom certificates. The MD5 hash of this Pegasus sample is 8468af0e577cae704ac059c025b932f8.
Strike Pegasus_c0c7cd31	This strike sends an Android malware sample known as Pegasus. It is a spyware developed by the NSO group which exfiltrates data from installed social media apps, steals stored credentials, takes screenshots, photos and many more malicious activities. NOTE: The APK samples have been signed with custom certificates. The MD5 hash of this Pegasus sample is c0c7cd3173ceb9b666a7424f5b860b50.
Strike Pegasus_cc9517aa	This strike sends an Android malware sample known as Pegasus. It is a spyware developed by the NSO group which exfiltrates data from installed social media apps, steals stored credentials, takes screenshots, photos and many more malicious activities. The MD5 hash of this Pegasus sample is cc9517aafb58279091ac17533293edc1.
Strike Pegasus_d0ce7423	This strike sends an Android malware sample known as Pegasus. It is a spyware developed by the NSO group which exfiltrates data from installed social media apps, steals stored credentials, takes screenshots, photos and many more malicious activities. NOTE: The APK samples have been signed with custom certificates. The MD5 hash of this Pegasus sample is d0ce742309db73e797157045c58942b1.
Strike Pegasus_f1a6be3f	This strike sends an Android malware sample known as Pegasus. It is a spyware developed by the NSO group which exfiltrates data from installed social media apps, steals stored credentials, takes screenshots, photos and many more malicious activities. NOTE: The APK samples have been signed with custom certificates. The MD5 hash of this Pegasus sample is f1a6be3f6129e96331d1e5484bf0a625.

<b>Name</b>	<b>Description</b>
Strike PhantomNet_0fbc2bf2	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 0fbc2bf2f66fc72c521a9b8561bab1da.
Strike PhantomNet_1498f1df	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 1498f1df4ca0e9cf23babe00cf34ed3d.
Strike PhantomNet_2632fa8f	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 2632fa8fc67dd2fd5c5a6275465dcc95.
Strike PhantomNet_3b4ea607	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 3b4ea6079ac9f154e0d4ec2cb6d05431.
Strike PhantomNet_608877a9	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 608877a9e11101da53bce99b0effc75b.

<b>Name</b>	<b>Description</b>
Strike PhantomNet_66007a1c	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 66007a1ca6d07ebb4ed85bf82e79719d.
Strike PhantomNet_7de7febe	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 7de7feb6bed06c49efb4e2c3dd23e1.
Strike PhantomNet_81159738	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is 81159738f7ffb50d5bc3c75e5e0ac546.
Strike PhantomNet_b6e3894c	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is b6e3894c17fb05db754a61ac9a0e5925.
Strike PhantomNet_bbf9216	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is bbf92161cb71825a16e49e2aa4d2750.

<b>Name</b>	<b>Description</b>
Strike PhantomNet_f21b63dd	This strike sends a malware sample known as PhantomNet. PhantomNet is a malware of the backdoor type that provides a persistent presence on the targeted network. It is delivered through spear-phishing emails that direct users to malicious webpages designed to mimic legitimate ones, where an exploitation framework attempts to compromise visitors' browsers. The first-stage payload, Voxel, persistent on the system and maintains communication with a remote server controlled by the attacker. Its key capabilities include exfiltrating data, downloading and executing secondary payloads, and performing man-in-the-middle attacks. The MD5 hash of this PhantomNet sample is f21b63ddd7d2a773eb21a065015cdd01.
Strike Phoenix Cryptolocker_d86f451b	This strike sends a malware sample known as Phoenix Cryptolocker. Phoenix Cryptolocker is a ransomware that made headlines when it was detected in an attack against CNA Financial. The malware is able to infiltrate by appearing to be a legitimate utility and coming signed with a digital certificate. After infection and file encryption, the malware deletes all traces of itself leaving behind only the ransom note with instructions for the victim. The MD5 hash of this Phoenix Cryptolocker sample is d86f451bbff804e59a549f9fb33d6e3f.
Strike PixPirate_5948461c	This strike sends a polymorphic malware sample known as PixPirate. PixPirate is an Android banking Trojan designed to carry out Automatic Transfer System (ATS) attacks, primarily targeting Brazilian banks using the Pix Instant Payment platform. It intercepts and deletes SMS messages, prevents uninstallation, and conducts malvertising campaigns. Using Accessibility Services, PixPirate steals banking passwords, tailoring its approach to each targeted bank's application layout. 'com.turnip.index' is the package name of the malware sample. Constant strings in the code have been encrypted. The MD5 hash of this malware sample is 5948461cacbeb2543f52ac0a08161884.
Strike PixPirate_7d55da5e	This strike sends a polymorphic malware sample known as PixPirate. PixPirate is an Android banking Trojan designed to carry out Automatic Transfer System (ATS) attacks, primarily targeting Brazilian banks using the Pix Instant Payment platform. It intercepts and deletes SMS messages, prevents uninstallation, and conducts malvertising campaigns. Using Accessibility Services, PixPirate steals banking passwords, tailoring its approach to each targeted bank's application layout. 'com.turnip.index' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 7d55da5e52fbad590a0b472dabf57455.
Strike PixPirate_91b14bf2	This strike sends a polymorphic malware sample known as PixPirate. PixPirate is an Android banking Trojan designed to carry out Automatic Transfer System (ATS) attacks, primarily targeting Brazilian banks using the Pix Instant Payment platform. It intercepts and deletes SMS messages, prevents uninstallation, and conducts malvertising campaigns. Using Accessibility Services, PixPirate steals banking passwords, tailoring its approach to each targeted bank's application layout. 'com.simplicity.transformer' is the package name of the malware sample. Constant strings in the code have been encrypted. The MD5 hash of this malware sample is 91b14bf2b8c4a588fdf7f37e6c79b3fd.

<b>Name</b>	<b>Description</b>
Strike PixPirate_921c1955	This strike sends a polymorphic malware sample known as PixPirate. PixPirate is an Android banking Trojan designed to carry out Automatic Transfer System (ATS) attacks, primarily targeting Brazilian banks using the Pix Instant Payment platform. It intercepts and deletes SMS messages, prevents uninstallation, and conducts malvertising campaigns. Using Accessibility Services, PixPirate steals banking passwords, tailoring its approach to each targeted bank's application layout. 'com.simplicity.transformer' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 921c1955f79bc3c69db8c61147226de2.
Strike PixPirate_93a2b43f	This strike sends a malware sample known as PixPirate. PixPirate is an Android banking Trojan designed to carry out Automatic Transfer System (ATS) attacks, primarily targeting Brazilian banks using the Pix Instant Payment platform. It intercepts and deletes SMS messages, prevents uninstallation, and conducts malvertising campaigns. Using Accessibility Services, PixPirate steals banking passwords, tailoring its approach to each targeted bank's application layout. 'com.simplicity.transformer' is the package name of the malware sample. The MD5 hash of this malware sample is 93a2b43f862013f8c50393443ec6497a.
Strike PixPirate_c382d8e5	This strike sends a malware sample known as PixPirate. PixPirate is an Android banking Trojan designed to carry out Automatic Transfer System (ATS) attacks, primarily targeting Brazilian banks using the Pix Instant Payment platform. It intercepts and deletes SMS messages, prevents uninstallation, and conducts malvertising campaigns. Using Accessibility Services, PixPirate steals banking passwords, tailoring its approach to each targeted bank's application layout. 'com.turnip.index' is the package name of the malware sample. The MD5 hash of this malware sample is c382d8e5f2aaa033521a9310d23461c7.
Strike PixPirate_e12030f6	This strike sends a polymorphic malware sample known as PixPirate. PixPirate is an Android banking Trojan designed to carry out Automatic Transfer System (ATS) attacks, primarily targeting Brazilian banks using the Pix Instant Payment platform. It intercepts and deletes SMS messages, prevents uninstallation, and conducts malvertising campaigns. Using Accessibility Services, PixPirate steals banking passwords, tailoring its approach to each targeted bank's application layout. 'com.simplicity.transformer' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is e12030f67003a7009d51bd0e86f6f6c7.
Strike PixPirate_e334ad17	This strike sends a polymorphic malware sample known as PixPirate. PixPirate is an Android banking Trojan designed to carry out Automatic Transfer System (ATS) attacks, primarily targeting Brazilian banks using the Pix Instant Payment platform. It intercepts and deletes SMS messages, prevents uninstallation, and conducts malvertising campaigns. Using Accessibility Services, PixPirate steals banking passwords, tailoring its approach to each targeted bank's application layout. 'com.turnip.index' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is e334ad176c31e74c66dca3e1099da574.

<b>Name</b>	<b>Description</b>
Strike PteroLNK_17292f18	<p>This strike sends a malware sample known as PteroLNK. This strike sends a malware sample known as PteroLNK. PteroLNK is a VBScript-based loader used in cyberespionage campaigns attributed to the Russian-linked Gamaredon threat group. It is delivered through obfuscated scripts that deploy additional components, including a downloader and an LNK dropper. The downloader retrieves command and control infrastructure via Dead Drop Resolvers hosted on services like Telegraph and Teletype, while the LNK dropper creates malicious shortcuts across local and network drives to trigger payload execution. The malware achieves persistence through scheduled tasks, uses obfuscation and environment checks to evade detection, and communicates with its C2 using Cloudflare tunnels and machine-specific User-Agent headers. The MD5 hash of this PteroLNK sample is 17292f18012dbb863e9945fc434e6e48.</p>
Strike PteroLNK_405e482f	<p>This strike sends a malware sample known as PteroLNK. This strike sends a malware sample known as PteroLNK. PteroLNK is a VBScript-based loader used in cyberespionage campaigns attributed to the Russian-linked Gamaredon threat group. It is delivered through obfuscated scripts that deploy additional components, including a downloader and an LNK dropper. The downloader retrieves command and control infrastructure via Dead Drop Resolvers hosted on services like Telegraph and Teletype, while the LNK dropper creates malicious shortcuts across local and network drives to trigger payload execution. The malware achieves persistence through scheduled tasks, uses obfuscation and environment checks to evade detection, and communicates with its C2 using Cloudflare tunnels and machine-specific User-Agent headers. The MD5 hash of this PteroLNK sample is 405e482fb991c52326c64ed31c835e4d.</p>
Strike PteroLNK_7bbd6e73	<p>This strike sends a malware sample known as PteroLNK. This strike sends a malware sample known as PteroLNK. PteroLNK is a VBScript-based loader used in cyberespionage campaigns attributed to the Russian-linked Gamaredon threat group. It is delivered through obfuscated scripts that deploy additional components, including a downloader and an LNK dropper. The downloader retrieves command and control infrastructure via Dead Drop Resolvers hosted on services like Telegraph and Teletype, while the LNK dropper creates malicious shortcuts across local and network drives to trigger payload execution. The malware achieves persistence through scheduled tasks, uses obfuscation and environment checks to evade detection, and communicates with its C2 using Cloudflare tunnels and machine-specific User-Agent headers. The MD5 hash of this PteroLNK sample is 7bbd6e738305b01a1c77db755cf01053.</p>
Strike PteroLNK_7fb9ad48	<p>This strike sends a malware sample known as PteroLNK. This strike sends a malware sample known as PteroLNK. PteroLNK is a VBScript-based loader used in cyberespionage campaigns attributed to the Russian-linked Gamaredon threat group. It is delivered through obfuscated scripts that deploy additional components, including a downloader and an LNK dropper. The downloader retrieves command and control infrastructure via Dead Drop Resolvers hosted on services like Telegraph and Teletype, while the LNK dropper creates malicious shortcuts across local and network drives to trigger payload execution. The malware achieves persistence through scheduled tasks, uses obfuscation and environment checks to evade detection, and communicates with its C2 using Cloudflare tunnels and machine-specific User-Agent headers. The MD5 hash of this PteroLNK sample is 7fb9ad48766f77441b8389d6ff233409.</p>

<b>Name</b>	<b>Description</b>
Strike PteroLNK_817ba232	<p>This strike sends a malware sample known as PteroLNK. This strike sends a malware sample known as PteroLNK. PteroLNK is a VBScript-based loader used in cyberespionage campaigns attributed to the Russian-linked Gamaredon threat group. It is delivered through obfuscated scripts that deploy additional components, including a downloader and an LNK dropper. The downloader retrieves command and control infrastructure via Dead Drop Resolvers hosted on services like Telegraph and Teletype, while the LNK dropper creates malicious shortcuts across local and network drives to trigger payload execution. The malware achieves persistence through scheduled tasks, uses obfuscation and environment checks to evade detection, and communicates with its C2 using Cloudflare tunnels and machine-specific User-Agent headers. The MD5 hash of this PteroLNK sample is 817ba23224a66963e33d6eb2f9be63c4.</p>
Strike PteroLNK_850124cc	<p>This strike sends a malware sample known as PteroLNK. This strike sends a malware sample known as PteroLNK. PteroLNK is a VBScript-based loader used in cyberespionage campaigns attributed to the Russian-linked Gamaredon threat group. It is delivered through obfuscated scripts that deploy additional components, including a downloader and an LNK dropper. The downloader retrieves command and control infrastructure via Dead Drop Resolvers hosted on services like Telegraph and Teletype, while the LNK dropper creates malicious shortcuts across local and network drives to trigger payload execution. The malware achieves persistence through scheduled tasks, uses obfuscation and environment checks to evade detection, and communicates with its C2 using Cloudflare tunnels and machine-specific User-Agent headers. The MD5 hash of this PteroLNK sample is 850124cca29c6034cf623ba8b09b7947.</p>
Strike PteroLNK_98cf1a95	<p>This strike sends a malware sample known as PteroLNK. This strike sends a malware sample known as PteroLNK. PteroLNK is a VBScript-based loader used in cyberespionage campaigns attributed to the Russian-linked Gamaredon threat group. It is delivered through obfuscated scripts that deploy additional components, including a downloader and an LNK dropper. The downloader retrieves command and control infrastructure via Dead Drop Resolvers hosted on services like Telegraph and Teletype, while the LNK dropper creates malicious shortcuts across local and network drives to trigger payload execution. The malware achieves persistence through scheduled tasks, uses obfuscation and environment checks to evade detection, and communicates with its C2 using Cloudflare tunnels and machine-specific User-Agent headers. The MD5 hash of this PteroLNK sample is 98cf1a959f11af59bd5ac2c2d746541f.</p>
Strike PteroLNK_b533defb	<p>This strike sends a malware sample known as PteroLNK. This strike sends a malware sample known as PteroLNK. PteroLNK is a VBScript-based loader used in cyberespionage campaigns attributed to the Russian-linked Gamaredon threat group. It is delivered through obfuscated scripts that deploy additional components, including a downloader and an LNK dropper. The downloader retrieves command and control infrastructure via Dead Drop Resolvers hosted on services like Telegraph and Teletype, while the LNK dropper creates malicious shortcuts across local and network drives to trigger payload execution. The malware achieves persistence through scheduled tasks, uses obfuscation and environment checks to evade detection, and communicates with its C2 using Cloudflare tunnels and machine-specific User-Agent headers. The MD5 hash of this PteroLNK sample is b533defb9566adf1cd2244bcf235ef8a.</p>

<b>Name</b>	<b>Description</b>
Strike PteroLNK_bd9038f2	<p>This strike sends a malware sample known as PteroLNK. This strike sends a malware sample known as PteroLNK. PteroLNK is a VBScript-based loader used in cyberespionage campaigns attributed to the Russian-linked Gamaredon threat group. It is delivered through obfuscated scripts that deploy additional components, including a downloader and an LNK dropper. The downloader retrieves command and control infrastructure via Dead Drop Resolvers hosted on services like Telegraph and Teletype, while the LNK dropper creates malicious shortcuts across local and network drives to trigger payload execution. The malware achieves persistence through scheduled tasks, uses obfuscation and environment checks to evade detection, and communicates with its C2 using Cloudflare tunnels and machine-specific User-Agent headers. The MD5 hash of this PteroLNK sample is bd9038f263e5b843f57e4fbbe971447.</p>
Strike PteroLNK_fdb65842	<p>This strike sends a malware sample known as PteroLNK. This strike sends a malware sample known as PteroLNK. PteroLNK is a VBScript-based loader used in cyberespionage campaigns attributed to the Russian-linked Gamaredon threat group. It is delivered through obfuscated scripts that deploy additional components, including a downloader and an LNK dropper. The downloader retrieves command and control infrastructure via Dead Drop Resolvers hosted on services like Telegraph and Teletype, while the LNK dropper creates malicious shortcuts across local and network drives to trigger payload execution. The malware achieves persistence through scheduled tasks, uses obfuscation and environment checks to evade detection, and communicates with its C2 using Cloudflare tunnels and machine-specific User-Agent headers. The MD5 hash of this PteroLNK sample is fdb658425059ad21fb0b84f3e03dcd2e.</p>
Strike PuTTYRider_02b3a5f0	<p>This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is 02b3a5f0121fab02f22173c9e738fee6.</p>
Strike PuTTYRider_0e041de4	<p>This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is 0e041de4bca18fdfa54c525ae524e018.</p>
Strike PuTTYRider_4e61cfa7	<p>This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is 4e61cfa7d791788ae557319e83c63fb4.</p>

<b>Name</b>	<b>Description</b>
Strike PuTTYRider_7b1854a4	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is 7b1854a4bd691db129459ac6f50668b6.
Strike PuTTYRider_8eb873ad	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is 8eb873ad112121cdfd0cc72688aa229f.
Strike PuTTYRider_8ed690f6	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is 8ed690f6438133f4661465253daba3bc.
Strike PuTTYRider_93b46063	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is 93b460635a4015d04bfae9eb3cd537cc.
Strike PuTTYRider_bb50383e	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is bb50383eac05377d7feae5b9c3024550.

<b>Name</b>	<b>Description</b>
Strike PuTTYRider_e48431ba	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is e48431ba5aa7a42ae0a32eb7d859d7a4.
Strike PuTTYRider_eb119087	This strike sends a malware sample known as PuTTYRider. PuTTYRider is a malware that is delivered through weaponized PuTTY applications. It is propagated via Bing Ads that lead to a download of the modified version of PuTTY. Once the user downloads and executes the malicious PuTTY version, it installs a backdoor that allows unauthorized access to the victim's system. Its key capabilities include remote access, data exfiltration, and providing the attacker with full control over the compromised system. The MD5 hash of this PuTTYRider sample is eb119087d7395ca0e9c32e5fc3bc3b.
Strike PyXie Lite_111019f2	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is 111019f2333c79cd320b3acc474df34c.
Strike PyXie Lite_127aa359	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is 127aa359a279cb299b63bb720f35ed1d.
Strike PyXie Lite_36ae75fd	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is 36ae75fd0c0afc7d6503f66880d6acf8.
Strike PyXie Lite_38bb2a24	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is 38bb2a242823592548a6c6539d69e72a.
Strike PyXie Lite_49819f0e	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is 49819f0eee4399ea309d83fea14acb69.

<b>Name</b>	<b>Description</b>
Strike PyXie Lite_57142545	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is 571425452e7fa287ce283a4a4b479ff1.
Strike PyXie Lite_78038fcb	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is 78038fcb760ec0d4a446e243f496f026.
Strike PyXie Lite_8357b481	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is 8357b48174b91644012b7969d2ae9597.
Strike PyXie Lite_86d297b2	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is 86d297b262fb1e9f8c1cee271ceea40e.
Strike PyXie Lite_a76db545	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is a76db545952dcb01bdb966e656c3bac.
Strike PyXie Lite_ab109ced	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is ab109ced41f9be476da69b671d4e28ce.
Strike PyXie Lite_af27bf67	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is af27bf67e462bf5ef61b15a0e160ea84.
Strike PyXie Lite_d0857462	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is d0857462281df296b60a8814d4fa052f.

<b>Name</b>	<b>Description</b>
Strike PyXie Lite_e4940335	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is e4940335c81b5bcd4713ad929027077e.
Strike PyXie Lite_ed784123	This strike sends a malware sample known as PyXie Lite. PyXie Lite is a variant of its predecessor PyXie, the Python RAT. It can be recognized by its much smaller code base and a few other noticeable changes in its functionality, which include a hardened interpreter, remapped opcode table, exfiltration of data through internal servers, and performing reconnaissance. The MD5 hash of this PyXie Lite sample is ed784123007890e3df70b2348779b007.
Strike PyXie RAT_1856d7d2	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is 1856d7d2a60bfc2da5c36781294e5033.
Strike PyXie RAT_1955375a	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is 1955375a3ba47f2d293aad78e2478edf.
Strike PyXie RAT_1cae93d1	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is 1cae93d1e1ab2e6bb1db8b65d374b785.
Strike PyXie RAT_2aac1415	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is 2aac141539e4bac0320ce3992e632d97.
Strike PyXie RAT_3b8c4e9f	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is 3b8c4e9f27a265c2ba4c39ee94e135a2.
Strike PyXie RAT_3d89a7df	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is 3d89a7dfd0984f23c4ebd1931d029108.

<b>Name</b>	<b>Description</b>
Strike PyXie RAT_4201d768	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is 4201d7681dbbde038de0e5d3568363da.
Strike PyXie RAT_440c46ac	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is 440c46ace55eb539376c05dc03e98cd4.
Strike PyXie RAT_4d9e184b	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is 4d9e184b5e67c83a4a9901ee43232934.
Strike PyXie RAT_4eab4038	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is 4eab40382656af8fa25fb23b6e6473a0.
Strike PyXie RAT_54c11dcb	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is 54c11dcb706996a76976211c3685153d.
Strike PyXie RAT_5d2fd364	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is 5d2fd364769d12d26c83922e5e31e48e.
Strike PyXie RAT_837dda01	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is 837dda0135b0aa7628874b451c66b50f.
Strike PyXie RAT_9d3e1289	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is 9d3e12893fae7eb6c33682b5bbea6d93.
Strike PyXie RAT_a07761d3	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is a07761d3be0749c5ba7da3d8222f1d86.

<b>Name</b>	<b>Description</b>
Strike PyXie RAT_a7da1675	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is a7da167512ae0077122e349e1cf54085.
Strike PyXie RAT_aa03fbdd	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is aa03fbbd932b6f57d26c53cf7a01ef1b.
Strike PyXie RAT_aa64323c	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is aa64323c466ac0ae62ec6532bac30936.
Strike PyXie RAT_cf1ad0f6	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is cf1ad0f6c0f7dfe7b5940008ed27bc28.
Strike PyXie RAT_d76837f8	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is d76837f88a8d62351e2d551be2fe9893.
Strike PyXie RAT_f198217b	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is f198217bafc00828a2f5bc7f816c8e1d.
Strike PyXie RAT_fa8a1311	This strike sends a malware sample known as PyXie RAT. PyXie is a Python Remote Access Trojan. It has been seen in the wild since 2018, and is typically seen in conjunction with Cobalt Strike beacons. PyXie has been used to deliver ransomware attacks to the healthcare and education industries. The MD5 hash of this PyXie RAT sample is fa8a1311b6488e40de471cc183ce50eb.
Strike PylangGhost_02476bc3	This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1 Password. The MD5 hash of this PylangGhost sample is 02476bc333be305bd0f5791d389755cd.

<b>Name</b>	<b>Description</b>
Strike PylangGhost_137c04d5	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is 137c04d5f0733b3780b20927185480d2.</p>
Strike PylangGhost_14400ffd	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is 14400ffd64ebfe27586814f46dd9ab32.</p>
Strike PylangGhost_29c40163	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is 29c4016315b653c2a1eacb84c932fad1.</p>
Strike PylangGhost_3d62d69e	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is 3d62d69e5bc96ae100b6a98182745841.</p>

<b>Name</b>	<b>Description</b>
Strike PylangGhost_400f8582	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is 400f8582ea4c8d9173f28685b0d744fd.</p>
Strike PylangGhost_50992b4e	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is 50992b4ede8a9d2e59dfda184e5c68a4.</p>
Strike PylangGhost_5591b1c6	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is 5591b1c680aac1be0a51a450da687ee7.</p>
Strike PylangGhost_68b344a9	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is 68b344a965f24239211de8c3cc53247f.</p>

<b>Name</b>	<b>Description</b>
Strike PylangGhost_6db2a64d	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is 6db2a64d9653c1ddba7fce701b09bfe8.</p>
Strike PylangGhost_923d805e	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is 923d805e759af84632bd5c85bedbc57e.</p>
Strike PylangGhost_94bcfc0a	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is 94bcfc0a783258c3111e0a3b0f450c91.</p>
Strike PylangGhost_9f1acef5	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is 9f1acef5a7909bb9ac5ffdef90b3fb4f.</p>

<b>Name</b>	<b>Description</b>
Strike PylangGhost_a794992f	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is a794992f98cd3da70e0abf1ac3d50aa0.</p>
Strike PylangGhost_c3a1bfc4	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is c3a1bfc4df71b0053a0f98e891a7c3d6.</p>
Strike PylangGhost_cdd693e0	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is cdd693e00d4000db284fd13faa481134.</p>
Strike PylangGhost_e4def2aa	<p>This strike sends a malware sample known as PylangGhost. This strike sends a malware sample known as PylangGhost. PylangGhost is a Python-based remote access trojan (RAT) and a variant of the GolangGhost malware, linked to the North Korean-aligned threat actor Famous Chollima. It is distributed through phishing campaigns that impersonate job interview processes, tricking victims into executing a malicious ClickFix utility. Once launched on Windows systems, the malware establishes persistence via registry modifications and connects to a C2 server using RC4-encrypted HTTP communication. It enables attackers to execute remote shell commands, transfer files, and steal data, including credentials and browser extension information from over 80 wallet and password managers such as MetaMask and 1Password. The MD5 hash of this PylangGhost sample is e4def2aa4d18d3e6ad6922446f68366c.</p>

<b>Name</b>	<b>Description</b>
Strike Qakbot_083ac8b9	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 083ac8b93aabdd9c11c15cc2e279d6f0.
Strike Qakbot_083f147f	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 083f147f6795d0421a923b6786178992.
Strike Qakbot_09b8fe17	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 09b8fe179666a8bd4aa193169aa138c1.
Strike Qakbot_10fb7039	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 10fb7039d24f8593a7de808f8204ead1.
Strike Qakbot_11a1f578	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 11a1f578e4f9f2b621b8be07345c05bb.
Strike Qakbot_1330fdb5	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 1330fdb5121c445cb1bad6a2d04df63e.
Strike Qakbot_140712ed	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 140712ed211d973de5a3274608cf28c0.
Strike Qakbot_19a9f5b3	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 19a9f5b3b34b6ee7cf218de98aa87df2.
Strike Qakbot_1b7f60cd	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 1b7f60cd44c6a084aa5144a1a119a5e2.

<b>Name</b>	<b>Description</b>
Strike Qakbot_1f9f0f4c	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 1f9f0f4c322ed6979514222f12915d5f.
Strike Qakbot_203699e7	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 203699e7484d7c46a2c545a19b31f614.
Strike Qakbot_21196344	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 21196344f852f24d07655779e2205da3.
Strike Qakbot_21745986	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 21745986c938cf7ce19211df7bc2217d.
Strike Qakbot_2189e297	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 2189e297d1900f7766d07be488c05502.
Strike Qakbot_291b6ad9	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 291b6ad955a0d64fae7c9aafbef2ac5e.
Strike Qakbot_29d55386	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 29d55386b42ae4f7029533b3e7d79d19.
Strike Qakbot_2a72139e	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 2a72139e1ac6bca1109205fe92d6d5ce.
Strike Qakbot_2b6aef0d	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 2b6aef0dde3e3ca606b12a7076f9e486.

<b>Name</b>	<b>Description</b>
Strike Qakbot_2e360a71	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 2e360a714d2cebeb1b0055b16cff0d7e.
Strike Qakbot_32608fee	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 32608fee5f14e3733f1367a95abcf569.
Strike Qakbot_33776586	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 3377658676ee4e666ba077ccda5f93bc.
Strike Qakbot_3f774b7e	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 3f774b7e5eb656c1e174b9d3f3003e79.
Strike Qakbot_3f7f4d66	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 3f7f4d669ff9f912a8bceafc89f2b924.
Strike Qakbot_3ffe5601	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 3ffe560127804443b98953de7c9dd5fa.
Strike Qakbot_40155b0f	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 40155b0fba5d52eb6c3dc9b1164e6404.
Strike Qakbot_4036ff97	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 4036ff97f2229b2262f95014bf58df9b.
Strike Qakbot_405dc314	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 405dc3140fd0f010ff08a3b5b7833158.

<b>Name</b>	<b>Description</b>
Strike Qakbot_412af7b4	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 412af7b412d0b758a78c788e48d480bd.
Strike Qakbot_42284715	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 42284715939561b2992346faaaeef610.
Strike Qakbot_483e3c71	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 483e3c7176a7e5e4445651c6fe824abb.
Strike Qakbot_4989af5b	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 4989af5b16f7fdb9de808337dbdc0b3a.
Strike Qakbot_4c08497d	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 4c08497dcc46ef0bb965a34d9e5fd32c.
Strike Qakbot_4f2e59b6	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 4f2e59b6050e873fd41a0b369b354243.
Strike Qakbot_4f65cf53	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 4f65cf53d8d47db9b7af0b66ec131052.
Strike Qakbot_502752a6	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 502752a6d7496027cf5dc9612bff5902.
Strike Qakbot_510668ce	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 510668ce687bb7529868501eabdcca35.

<b>Name</b>	<b>Description</b>
Strike Qakbot_52575508	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 5257550892a72d7bec8a4e2c20fd106d.
Strike Qakbot_531911a3	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 531911a31393a80fc654597d2e7b3abb.
Strike Qakbot_53c3ad17	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 53c3ad170d9b83f584696e7f5507d7e3.
Strike Qakbot_55abb44e	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 55abb44e737b2a7a27b0f424bb5d2ba5.
Strike Qakbot_5b656068	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 5b6560682dbd9b107b0b8d3acb1f6267.
Strike Qakbot_5ba7f847	This strike sends a polymorphic malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The binary has the checksum removed in the PE file format. The MD5 hash of this Qakbot sample is 5ba7f847655bb5bec39f148edfc75db0.
Strike Qakbot_5c00db17	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 5c00db1760ffd163c86597a1ac93a20b.
Strike Qakbot_5d84230a	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 5d84230aa0c14a853c381a5e1b2628ba.

<b>Name</b>	<b>Description</b>
Strike Qakbot_5d9021e8	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 5d9021e84a65f0a294b1a8540f54ead0.
Strike Qakbot_5df167f3	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 5df167f3192b8e23833a0a5f8d2fca45.
Strike Qakbot_5e48d9b9	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 5e48d9b9341030080107f977b9ce9263.
Strike Qakbot_5f428832	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 5f4288328492c707e1d6398224417a27.
Strike Qakbot_61160311	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 6116031131838e58dbd0a5fab585a850.
Strike Qakbot_61847aec	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 61847aec901fcbb00992d7563f026e5d.
Strike Qakbot_620bda71	This strike sends a polymorphic malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The binary has the checksum removed in the PE file format. The MD5 hash of this Qakbot sample is 620bda711e7c51e6451af5d75de1c7f9.
Strike Qakbot_6325ecf7	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 6325ecf747a8c65a7ffc791aa524372f.

<b>Name</b>	<b>Description</b>
Strike Qakbot_65e20699	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 65e206996470de6b6a4d5a69e3e35848.
Strike Qakbot_66968cc4	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 66968cc4e332302d209835da2476c635.
Strike Qakbot_672e642a	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 672e642af35cac2735e19f1e488be72f.
Strike Qakbot_6a65ec4b	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 6a65ec4b09b37ebdedfee5d38ffa1cbe.
Strike Qakbot_6bac5b97	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 6bac5b97ef676e137e35e393917fab90.
Strike Qakbot_6d3979c8	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 6d3979c8ad1fc378ca751e8b978a941b.
Strike Qakbot_6f149572	This strike sends a polymorphic malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Qakbot sample is 6f1495721e6f5576a8d076571f84df47.
Strike Qakbot_6f9f39ee	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 6f9f39eea7e555d4167cf1969cd0303b.

<b>Name</b>	<b>Description</b>
Strike Qakbot_70011104	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 70011104f678ba095188b3975d29aa6b.
Strike Qakbot_73c5c9c0	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 73c5c9c056a12cd9ea3d4976f90a1757.
Strike Qakbot_75c711af	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 75c711afcbde3ff9095f53eb30bd1961.
Strike Qakbot_76f0cfb3	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 76f0cfb3c8143fe677dae170a9804c66.
Strike Qakbot_788bc825	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 788bc82511b7723999a30c01213ad702.
Strike Qakbot_81727d8d	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 81727d8da0a344fe77ae4877e7df28fa.
Strike Qakbot_82189898	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 82189898694af9b8e5ea9058da56261e.
Strike Qakbot_82ae9fa9	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 82ae9fa967a854b3c015cac619909e5c.
Strike Qakbot_84b16649	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 84b16649c3a9459bda8d645f37487cc2.

<b>Name</b>	<b>Description</b>
Strike Qakbot_85d4e77b	This strike sends a polymorphic malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The binary has the checksum removed in the PE file format. The MD5 hash of this Qakbot sample is 85d4e77b12ae4eb3e9ed09c98fa44d86.
Strike Qakbot_86c75973	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 86c7597356d5b2a7e1c664b83d703efd.
Strike Qakbot_8a6837b6	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 8a6837b631b6b816867a216174b8a004.
Strike Qakbot_8bce4f4e	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 8bce4f4e3645629b2effb384a711c780.
Strike Qakbot_8c6445de	This strike sends a polymorphic malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Qakbot sample is 8c6445de424b22dfb3339f5dea072156.
Strike Qakbot_8e3e0077	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 8e3e0077e1b79188117ad9bc7115ef2e.
Strike Qakbot_8f46946b	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 8f46946bc6fe6cd5843ca93c5b7d3045.
Strike Qakbot_906e7e71	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 906e7e7182eef7c85a0d3ebe8283ae36.

<b>Name</b>	<b>Description</b>
Strike Qakbot_90e2e4a4	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 90e2e4a4174e2619610a512c885c85de.
Strike Qakbot_91257224	This strike sends a polymorphic malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Qakbot sample is 91257224c05e3e3d8c1ee8d7fe014a91.
Strike Qakbot_925bb382	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 925bb382d450c773a5585ccdf6f13884.
Strike Qakbot_93c6b502	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 93c6b50240c4e7c220c55de4e12430ac.
Strike Qakbot_94cdc6bd	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 94cdc6bdf1021e5a632018c13d2cb5b7.
Strike Qakbot_988e391a	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 988e391a7bd88b2d362e44d57e97a778.
Strike Qakbot_98fa0cbd	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 98fa0cbdbeda2acad3efb8a5eeeeed562.
Strike Qakbot_9d0ed878	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 9d0ed8785c88f732ebfc7d11637a57c7.

<b>Name</b>	<b>Description</b>
Strike Qakbot_9d2cc830	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 9d2cc830c3a133a74ca6d83d6985200a.
Strike Qakbot_9e4bb7c2	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 9e4bb7c2bff8cc4245bf1327e84f125b.
Strike Qakbot_9f45de46	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 9f45de469dd7fec59078d0fd0a76b033.
Strike Qakbot_9f6694b9	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is 9f6694b96f990422ec0c4dd87497528b.
Strike Qakbot_9f8e8dd6	This strike sends a polymorphic malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Qakbot sample is 9f8e8dd6c3b95d095fd39687b2b6a0b.
Strike Qakbot_a290eda0	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is a290eda0a5a565042e2019ddc51610e9.
Strike Qakbot_a2f1f09d	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is a2f1f09d1bbe5bfc8630fab2187811ee.
Strike Qakbot_a3d6462c	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is a3d6462cdc162149e22502c694a7427c.

<b>Name</b>	<b>Description</b>
Strike Qakbot_a683a2f7	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is a683a2f746b192a4a2dd8e8fa683c714.
Strike Qakbot_a6a519b1	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is a6a519b1a8f2fc8372378513fbe3096f.
Strike Qakbot_a896b96a	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is a896b96a31d0ece9e401e1d77b7d6567.
Strike Qakbot_aaf9db74	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is aaf9db74093b270f8742864361ba3a45.
Strike Qakbot_aea860a2	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is aea860a2c9b5de2e6a9619affef59ab6.
Strike Qakbot_b0ffde08	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is b0ffde08f15d2543caf52fc8863efbca.
Strike Qakbot_b2f82fff	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is b2f82fffaf5edbbc741cc7423c54a204.
Strike Qakbot_b4675efb	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is b4675efb7af833494f30356b6d8e6578.
Strike Qakbot_b6f8b13c	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is b6f8b13c020450d5218ed523754b1b56.

<b>Name</b>	<b>Description</b>
Strike Qakbot_b6fe7585	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is b6fe75856f1a56f07ce15fd332c41e6e.
Strike Qakbot_b78d07e0	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is b78d07e05cd8716afc4c929b8b810033.
Strike Qakbot_ba811d0b	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is ba811d0b025160b8c7766be010784dca.
Strike Qakbot_bb30456f	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is bb30456f5d7fc93307e9e82061fe0f8b.
Strike Qakbot_bd56adc8	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is bd56adc8c75c6973351981b24f1be32d.
Strike Qakbot_bf043150	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is bf043150b6bd4a1dadffda1b1a18d8eb.
Strike Qakbot_c1a91d62	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is c1a91d62c48fb71cbebda4011e6ae38.
Strike Qakbot_c2854d54	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is c2854d54350aeeaa8ff69da1435832ed.
Strike Qakbot_c31c0436	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is c31c0436a53ccc0d10da3f42a3605451.

<b>Name</b>	<b>Description</b>
Strike Qakbot_c378ead9	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is c378ead9fe62c17f0124b12246d9057b.
Strike Qakbot_c5353783	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is c5353783f4e722c9cdc065107a47e62f.
Strike Qakbot_c579791b	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is c579791b7d102d18967aa4bf05f28281.
Strike Qakbot_c611fb97	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is c611fb978592e9b1357244627049350d.
Strike Qakbot_c6404685	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is c640468581a747f755c21a044bd30f77.
Strike Qakbot_c7d27858	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is c7d27858519a1edad84d9560693b5b36.
Strike Qakbot_cd76cab9	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is cd76cab9e70999010d4549f660024bfe.
Strike Qakbot_cf2bc340	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is cf2bc34058f6e9684f0851a5fb0b59c7.
Strike Qakbot_cfd78095	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is cfd7809538b65db8f8d3fdbd645b93e03.

<b>Name</b>	<b>Description</b>
Strike Qakbot_d1ac9de4	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is d1ac9de4eee4cf5ca78ef82cac24190a.
Strike Qakbot_d2715637	This strike sends a polymorphic malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Qakbot sample is d2715637f4f9a631de611b64fa57ca82.
Strike Qakbot_d647b7bb	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is d647b7bb5d864949249f51d1a7927b47.
Strike Qakbot_d7d6b087	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is d7d6b087e5fb0450a0fb8c747850489.
Strike Qakbot_d8053079	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is d80530792140cbc13f6d21021e6c195.
Strike Qakbot_d867d6d9	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is d867d6d9a9b8a1fdf2467f27088f5230.
Strike Qakbot_da3b944d	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is da3b944da04513346d8ed4304fefc1.
Strike Qakbot_da8ab69a	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is da8ab69a032a706a1ba7b0ed620d79c3.

<b>Name</b>	<b>Description</b>
Strike Qakbot_dbb7ecb8	This strike sends a polymorphic malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The binary has random bytes appended at the end of the file. The MD5 hash of this Qakbot sample is dbb7ecb89e18360dd41a60adf94587ec.
Strike Qakbot_dc657bb8	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is dc657bb85a7c7f5bca74b99e6dfd72c9.
Strike Qakbot_e0c23898	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is e0c23898f4acf8a0fae7b430a3891b62.
Strike Qakbot_e0f2fec0	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is e0f2fec052912f010cb1d82d348d7e31.
Strike Qakbot_e306de36	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is e306de36207f82ad7fc0bf5026429e64.
Strike Qakbot_e5a95f5f	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is e5a95f5f45d3afdf9f3d0f27692def5.
Strike Qakbot_ecd95a8b	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is ecd95a8bfe2510b6591a9d1d23defcb0.
Strike Qakbot_f0d0539e	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is f0d0539ec7c89476a77c629d03014694.

<b>Name</b>	<b>Description</b>
Strike Qakbot_f1099c69	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is f1099c69a48cc7e974b0e5425a24504e.
Strike Qakbot_f194ecd8	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is f194ecd846a7214d6e45eda6df5b80c1.
Strike Qakbot_f1f9f5bb	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is f1f9f5bb60f4ea8ccf648f8d23dc29ed.
Strike Qakbot_f36c3faa	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is f36c3faa276a50373ad163bc5d3f8fe0.
Strike Qakbot_f64eb422	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is f64eb422a75b24a5c17652170378be83.
Strike Qakbot_fbfeeb0b	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is fbfeeb0b6db7c4d9d9dec9a296581de8.
Strike Qakbot_fc1fdfb4	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is fc1fdfb4cdda0f41bfb255359e442568.
Strike Qakbot_ff991ded	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is ff991ded540231f8e9a394c66ff13cad.
Strike Qakbot_ffe354bf	This strike sends a malware sample known as Qakbot. Qakbot, aka Qbot, has been around for since at least 2008. Qbot primarily targets sensitive information like banking credentials but can also steal FTP credentials and spread across a network using SMB. The MD5 hash of this Qakbot sample is ffe354bff028f1ddec7fb795dbd744ea.

<b>Name</b>	<b>Description</b>
Strike Qilin_0f73b467	This strike sends a malware sample known as Qilin. Qilin is a malware that is used in conjunction with other malicious software to carry out targeted attacks. It is usually delivered via spear-phishing emails or waterhole attacks, and is often seen in combination with the PlugX and Quasar RATs. Once executed, Qilin creates a backdoor into the infected system, allowing for further exploitation. Its key capabilities include launching additional payloads, achieving persistence, and performing reconnaissance on the infected system. The MD5 hash of this Qilin sample is 0f73b467ff03f9224c024f4eb3aecedb.
Strike Qilin_1c0cb55d	This strike sends a malware sample known as Qilin. Qilin is a malware that is used in conjunction with other malicious software to carry out targeted attacks. It is usually delivered via spear-phishing emails or waterhole attacks, and is often seen in combination with the PlugX and Quasar RATs. Once executed, Qilin creates a backdoor into the infected system, allowing for further exploitation. Its key capabilities include launching additional payloads, achieving persistence, and performing reconnaissance on the infected system. The MD5 hash of this Qilin sample is 1c0cb55d3a8d544ab0bd7d81d2985089.
Strike Qilin_227f14f4	This strike sends a malware sample known as Qilin. Qilin is a malware that is used in conjunction with other malicious software to carry out targeted attacks. It is usually delivered via spear-phishing emails or waterhole attacks, and is often seen in combination with the PlugX and Quasar RATs. Once executed, Qilin creates a backdoor into the infected system, allowing for further exploitation. Its key capabilities include launching additional payloads, achieving persistence, and performing reconnaissance on the infected system. The MD5 hash of this Qilin sample is 227f14f4c3aa35b9fb279f52c73b2e1e.
Strike Qilin_59c3334d	This strike sends a malware sample known as Qilin. Qilin is a malware that is used in conjunction with other malicious software to carry out targeted attacks. It is usually delivered via spear-phishing emails or waterhole attacks, and is often seen in combination with the PlugX and Quasar RATs. Once executed, Qilin creates a backdoor into the infected system, allowing for further exploitation. Its key capabilities include launching additional payloads, achieving persistence, and performing reconnaissance on the infected system. The MD5 hash of this Qilin sample is 59c3334d184159008cd45355b436d9a8.
Strike Qilin_bb8bdb3e	This strike sends a malware sample known as Qilin. Qilin is a malware that is used in conjunction with other malicious software to carry out targeted attacks. It is usually delivered via spear-phishing emails or waterhole attacks, and is often seen in combination with the PlugX and Quasar RATs. Once executed, Qilin creates a backdoor into the infected system, allowing for further exploitation. Its key capabilities include launching additional payloads, achieving persistence, and performing reconnaissance on the infected system. The MD5 hash of this Qilin sample is bb8bdb3e8c92e97e2f63626bc3b254c4.

<b>Name</b>	<b>Description</b>
Strike Qilin_e2c05908	This strike sends a malware sample known as Qilin. Qilin is a malware that is used in conjunction with other malicious software to carry out targeted attacks. It is usually delivered via spear-phishing emails or waterhole attacks, and is often seen in combination with the PlugX and Quasar RATs. Once executed, Qilin creates a backdoor into the infected system, allowing for further exploitation. Its key capabilities include launching additional payloads, achieving persistence, and performing reconnaissance on the infected system. The MD5 hash of this Qilin sample is e2c059083926ec2c219cebcfa4a49453.
Strike QuasarRAT_0554ce06	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 0554ce06b4125e7910a5eeab7dd7a630.
Strike QuasarRAT_056650c9	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this QuasarRAT sample is 056650c9d1938bd86d574771509a2abf.
Strike QuasarRAT_094dc708	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 094dc708a3feae65dab33f44c984b6f0.
Strike QuasarRAT_1347af31	This strike sends a malware sample known as QuasarRAT. On Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 1347af31f1f759cea0164dd26eeab53f.
Strike QuasarRAT_165309af	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 165309afb44362dd069f640c225fe8c3.

<b>Name</b>	<b>Description</b>
Strike QuasarRAT_1777246d	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 1777246de3428b757c2e4d4e9052b3e8.
Strike QuasarRAT_18d698fc	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has the timestamp field updated in the PE file header. The MD5 hash of this QuasarRAT sample is 18d698fc8ffe2818994d411d2edc89e7.
Strike QuasarRAT_18ea6c3f	This strike sends a malware sample known as QuasarRAT. On Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 18ea6c3f285a0609de3b4be052d26e99.
Strike QuasarRAT_1a2eca4f	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has random bytes appended at the end of the file. The MD5 hash of this QuasarRAT sample is 1a2eca4f46165b8a4047642cc5bcd79.
Strike QuasarRAT_1ab83ff9	This strike sends a malware sample known as QuasarRAT. On Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 1ab83ff93da4ce0da0fcb706f6bc8228.
Strike QuasarRAT_1d4a4ff2	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 1d4a4ff2adfa153b1035dd729c4f0bed.

<b>Name</b>	<b>Description</b>
Strike QuasarRAT_1ea755c0	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has the timestamp field updated in the PE file header. The MD5 hash of this QuasarRAT sample is 1ea755c0f9fea7bde48a62db3fc30e4a.
Strike QuasarRAT_25e35c28	This strike sends a malware sample known as QuasarRAT. On Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 25e35c28e0212a5c1e6c177be4d48b1a.
Strike QuasarRAT_2a8d7552	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this QuasarRAT sample is 2a8d7552b36e57aaa1bfa00abaf39d17.
Strike QuasarRAT_2aa82aa4	This strike sends a malware sample known as QuasarRAT. On Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 2aa82aa4c787c4f6299a22767d2ead47.
Strike QuasarRAT_2ac240b3	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 2ac240b39360eaf3ee309439b71d5e98.
Strike QuasarRAT_2c52c5ed	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has the timestamp field updated in the PE file header. The MD5 hash of this QuasarRAT sample is 2c52c5edd47b86f3a6aa21782cd3ec87.

<b>Name</b>	<b>Description</b>
Strike QuasarRAT_2dcc12bf	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 2dcc12bffd9566cfb1e7d78bb0fb9d4b.
Strike QuasarRAT_2e65ec5f	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this QuasarRAT sample is 2e65ec5ff812465296e3ad8ef4511428.
Strike QuasarRAT_36a4df9b	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this QuasarRAT sample is 36a4df9b0ab0f2d3a615f775d3dba9c0.
Strike QuasarRAT_3753a53a	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this QuasarRAT sample is 3753a53aea4d763ce54a0c65ba7382bc.
Strike QuasarRAT_3d92b0b9	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has the timestamp field updated in the PE file header. The MD5 hash of this QuasarRAT sample is 3d92b0b95ab85217746c2c8015526285.
Strike QuasarRAT_403b8d6a	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 403b8d6ab089c03181e2d5e32ea809fe.

<b>Name</b>	<b>Description</b>
Strike QuasarRAT_42660126	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 4266012612ff2990cc08534ea0fefd32.
Strike QuasarRAT_4803127b	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 4803127b429a1ed759c2b9709bd213bc.
Strike QuasarRAT_49423ccf	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 49423ccf65f8582c9c7ff7cab20ac285.
Strike QuasarRAT_4ac627ae	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this QuasarRAT sample is 4ac627ae8786300915337a8833e87824.
Strike QuasarRAT_4d80fa7c	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 4d80fa7c54645ad2d89c122a8ff4c00b.
Strike QuasarRAT_511d30b3	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this QuasarRAT sample is 511d30b3170d515982d85451255f2482.

<b>Name</b>	<b>Description</b>
Strike QuasarRAT_5d6f4a17	This strike sends a malware sample known as QuasarRAT. On Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 5d6f4a17539d84e07f978f808ceb877f.
Strike QuasarRAT_62db37de	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 62db37de46ba0bcca9411ba2a2a35827.
Strike QuasarRAT_68c08f0c	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this QuasarRAT sample is 68c08f0c831b24170da8cb0060be8642.
Strike QuasarRAT_68cc339e	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 68cc339ee818164424b8b383149fcad8.
Strike QuasarRAT_793a3daa	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this QuasarRAT sample is 793a3daa210d66facd326f6919d0545d.
Strike QuasarRAT_7978edcb	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 7978edcbad9f05433cc5ad31f5d789e5.

<b>Name</b>	<b>Description</b>
Strike QuasarRAT_7bec66ed	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 7bec66ed971abfbff9b25447a39fcaee.
Strike QuasarRAT_81ea33ae	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has random bytes appended at the end of the file. The MD5 hash of this QuasarRAT sample is 81ea33ae15c07aa80d3329c63e9fb1b5.
Strike QuasarRAT_85bb3da3	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has random bytes appended at the end of the file. The MD5 hash of this QuasarRAT sample is 85bb3da33068aa8b38124344ffc9b19b.
Strike QuasarRAT_8c18dae0	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has the timestamp field updated in the PE file header. The MD5 hash of this QuasarRAT sample is 8c18dae0cea12938476f51238ebc6eab.
Strike QuasarRAT_8d0e2631	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is 8d0e2631138907c09cf3f07f9c8aa26c.
Strike QuasarRAT_90f22ffd	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this QuasarRAT sample is 90f22ffd06c929d7b576dae1226abbe5.

<b>Name</b>	<b>Description</b>
Strike QuasarRAT_97398d7f	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has the timestamp field updated in the PE file header. The MD5 hash of this QuasarRAT sample is 97398d7f8cf3ecd255a79daa0688090b.
Strike QuasarRAT_99643fdd	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this QuasarRAT sample is 99643fddadefbf383c3541121edd2d6d7.
Strike QuasarRAT_a01d7c17	This strike sends a malware sample known as QuasarRAT. On Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is a01d7c171ed097992fa5ff6547d8c0fe.
Strike QuasarRAT_a0eab09b	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is a0eab09b2095854612d931e2bdb3280d.
Strike QuasarRAT_a242ae56	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is a242ae568af1fedc9d7540da878e817c.
Strike QuasarRAT_ab22a163	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is ab22a163f052e16dd29e5d1a1beae1e7.

<b>Name</b>	<b>Description</b>
Strike QuasarRAT_ae2833fc	This strike sends a malware sample known as QuasarRAT. On Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is ae2833fc5def4bebab9797e7694f8208.
Strike QuasarRAT_afae38a2	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is afae38a2c92cbec37c3ef6b1414e1f4e.
Strike QuasarRAT_b2880400	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is b288040040a839a5bffe8b5e1dc60a89.
Strike QuasarRAT_b349748b	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is b349748b015823ebd96917fed666f603.
Strike QuasarRAT_b7bd6ac3	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has random bytes appended at the end of the file. The MD5 hash of this QuasarRAT sample is b7bd6ac3f31f11a1330993773294c996.
Strike QuasarRAT_bc6f3340	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is bc6f33402000b952549176b98b8005b5.
Strike QuasarRAT_be896d1a	This strike sends a malware sample known as QuasarRAT. On Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is be896d1a70317c9e457fd3be91e54466.

<b>Name</b>	<b>Description</b>
Strike QuasarRAT_c5589254	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has random bytes appended at the end of the file. The MD5 hash of this QuasarRAT sample is c5589254f6eac99eb1f27b2ac71041e2.
Strike QuasarRAT_c8ec00d8	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has the timestamp field updated in the PE file header. The MD5 hash of this QuasarRAT sample is c8ec00d82b59bcfae34b249ac3892358.
Strike QuasarRAT_caf8166e	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is caf8166e2f177e5e40ddfb61f5140465.
Strike QuasarRAT_cc484d6f	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this QuasarRAT sample is cc484d6f5f4742f3a355567db9261d84.
Strike QuasarRAT_cc7d5e4b	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this QuasarRAT sample is cc7d5e4b2155c483ec3e3b4d71b871dc.
Strike QuasarRAT_cdd96af0	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is cdd96af015b85cf0a9279fa9b0af4454.

<b>Name</b>	<b>Description</b>
Strike QuasarRAT_ce004fd2	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this QuasarRAT sample is ce004fd23972989dcbcda5543c744f39.
Strike QuasarRAT_d957d99c	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is d957d99c41734479e375e58ff68dfdb2.
Strike QuasarRAT_dc96dcbd	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is dc96dcbd794bc860f109be49eb740896.
Strike QuasarRAT_e48ac0ab	This strike sends a malware sample known as QuasarRAT. On Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is e48ac0ab19c5b5599c45e9846ffb1de.
Strike QuasarRAT_e5f4b2c5	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is e5f4b2c5841de93eef284a02d0532c13.
Strike QuasarRAT_e7427799	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is e74277995df7ebf0aca7aa48f718c25d.

<b>Name</b>	<b>Description</b>
Strike QuasarRAT_ead5e826	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has random bytes appended at the end of the file. The MD5 hash of this QuasarRAT sample is ead5e82626333cf1195f1c58374edf64.
Strike QuasarRAT_f206ab0d	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is f206ab0defeb1bf6c9272d5b1a052985.
Strike QuasarRAT_fe7eb6b5	This strike sends a malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The MD5 hash of this QuasarRAT sample is fe7eb6b506959310e438d94910422c1c.
Strike QuasarRAT_ff5bd55c	This strike sends a polymorphic malware sample known as QuasarRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is QuasarRAT. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this QuasarRAT sample is ff5bd55cedfe5f35a62108bbd71cad99.
Strike QuirkyLoader_10e8d5ac	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 10e8d5ac2618249893621ed0a41352cc.
Strike QuirkyLoader_1b636f0a	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 1b636f0ac4cc6de7d4471e657335bf37.

<b>Name</b>	<b>Description</b>
Strike QuirkyLoader_26d4d38a	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 26d4d38a8f1d00fe4a1d62e300b98d80.
Strike QuirkyLoader_2c4da8bd	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 2c4da8bd3cbb9c94aa333bd5c576506b.
Strike QuirkyLoader_4116b369	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 4116b3691852c2c165e38b8af52ea578.
Strike QuirkyLoader_57868447	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 57868447d89fda05231bb6d9cf9bb8f.
Strike QuirkyLoader_6f071d1b	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 6f071d1b91536627b9ef8ea725b810fb.

<b>Name</b>	<b>Description</b>
Strike QuirkyLoader_74373fbc	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 74373fbce1940202e3cc0c25efbf90bf.
Strike QuirkyLoader_796f3de2	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 796f3de2f22819c86aefd4dab652522d.
Strike QuirkyLoader_8907fef4	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 8907fef409d8684cdd0c48043933aa0b.
Strike QuirkyLoader_99f78e41	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is 99f78e41cc5f086519626b8dfbb76f54.
Strike QuirkyLoader_b013e43b	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is b013e43be40c6c6608279f23733321b2.

<b>Name</b>	<b>Description</b>
Strike QuirkyLoader_b579d382	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is b579d3822cddd4babedc13ae9b786d3e.
Strike QuirkyLoader_e6b379aa	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is e6b379aa359195e02462ebd5fa1f1e9b.
Strike QuirkyLoader_eac607ad	This strike sends a malware sample known as QuirkyLoader. QuirkyLoader is a malware loader that delivers and deploys ransomware or other types of malware onto the victim computer. It uses a unique method of infection by embedding the malware into a .png file which is then delivered via phishing emails. Once the user opens the email and downloads the .png file, the malware is executed and starts deploying the payload. Its key capabilities include evasion of detection systems, downloading and executing additional payloads, and establishing persistent access to the infected system. The MD5 hash of this QuirkyLoader sample is eac607ad42e1e1b8dd9f7f85cc511ec3.
Strike Quishing_066a3d2a	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 066a3d2af563d058bf03aa85b41e03e1.
Strike Quishing_0e4b5632	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 0e4b56328a752449fae77124a3d5bda9.
Strike Quishing_18c75098	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 18c75098936560797ff0acd977210e54.
Strike Quishing_296e647d	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 296e647d3f13beceea7419570996620d.

<b>Name</b>	<b>Description</b>
Strike Quishing_31f3247b	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 31f3247b045c7b726ca4a22fcc2ae434.
Strike Quishing_452661d5	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 452661d506be7b0ba0ed183ea05d1fa9.
Strike Quishing_45f6524c	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 45f6524ca7371e0062f3d8ad502a5c82.
Strike Quishing_4cd09a89	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 4cd09a8914673fcbb1643ce6a1f4773e0.
Strike Quishing_5fdc03a5	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 5fdc03a5e6b83fd831f85e188bd9ee2a.
Strike Quishing_6f56c8f9	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 6f56c8f9587699edf39887238af3a284.
Strike Quishing_72cdb44a	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 72cdb44a2ffc3fbda04622373fefcce.
Strike Quishing_734e350f	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 734e350fc829523bd13311572618bdca.
Strike Quishing_7f1b3ee8	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 7f1b3ee81b42923b149cae7ff7b327e7.

<b>Name</b>	<b>Description</b>
Strike Quishing_95404201	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 95404201be191ba685b89a7b93e3631d.
Strike Quishing_9933302d	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 9933302d0f0e14d37947db7ef4989bdb.
Strike Quishing_9a5fbf54	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 9a5fbf54a3043a5d064bc4c96999bd5b.
Strike Quishing_9ffe2b8b	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is 9ffe2b8b25b3aa51b7dcb55fae4d7e77.
Strike Quishing_a316866b	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is a316866b8bddb8c519a210918c4df680.
Strike Quishing_a9ed09e2	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is a9ed09e295fd6c068faf71479bb1ca3b.
Strike Quishing_b66f8387	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is b66f838770ecf33f3dac578bee7229c2.
Strike Quishing_c1042440	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is c1042440af816dd25b555f2cf14a0f0a.
Strike Quishing_c33ab9ec	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is c33ab9ec8c33e065f3bd65113b1e16d5.

<b>Name</b>	<b>Description</b>
Strike Quishing_c69e577e	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is c69e577ea939c68d347e173d6dd80326.
Strike Quishing_cc7cdbce	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is cc7cdbced594dce769c03af65359a082.
Strike Quishing_cded9809	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is cded98091df8d54e9e95433965a8ca8b.
Strike Quishing_d54240c1	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is d54240c15d2815ec6df555d3762dd4e6.
Strike Quishing_dfde6ba6	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is dfde6ba6331945cff6ac1fdbc1e05c86.
Strike Quishing_e1e79771	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is e1e79771a6dcraf9cf957ed1e4b3d4b7e.
Strike Quishing_e39a2a9f	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is e39a2a9f5520df70056086be57114c99.
Strike Quishing_ec3f8803	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is ec3f8803fcb01c6cfa0dd2c5561103a2.
Strike Quishing_f733bc05	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is f733bc057c7026ef4ce5c6c2dd897194.

<b>Name</b>	<b>Description</b>
Strike Quishing_fa70f294	This strike sends a malware sample known as Quishing. Quishing or QR Code Phishing is a type of attack in which the attacker embeds the malicious URL inside a QR code. This sample is a pdf that contains a malicious QR code that uses social engineering to lure the victim to clicking malicious URLs. The MD5 hash of this Quishing sample is fa70f2949303fe442f3af01fda8ee624.
Strike QuiteRAT_0a2f5b41	This strike sends a polymorphic malware sample known as QuiteRAT. QuiteRAT is composed of Qt libraries. It is believed to belong to the MagicRAT family and although made up of Qt does not have a GUI. QuiteRAT has been detected in a campaign utilizing CVE-2022-47966 to deploy the RAT. The binary has random bytes appended at the end of the file. The MD5 hash of this QuiteRAT sample is 0a2f5b41bfad0e649fde2a6a30f6a264.
Strike QuiteRAT_365a5012	This strike sends a polymorphic malware sample known as QuiteRAT. QuiteRAT is composed of Qt libraries. It is believed to belong to the MagicRAT family and although made up of Qt does not have a GUI. QuiteRAT has been detected in a campaign utilizing CVE-2022-47966 to deploy the RAT. The binary has the timestamp field updated in the PE file header. The MD5 hash of this QuiteRAT sample is 365a50124e97acf2c758d7271bd2a046.
Strike QuiteRAT_3d5747d4	This strike sends a polymorphic malware sample known as QuiteRAT. QuiteRAT is composed of Qt libraries. It is believed to belong to the MagicRAT family and although made up of Qt does not have a GUI. QuiteRAT has been detected in a campaign utilizing CVE-2022-47966 to deploy the RAT. The binary has been packed using upx packer, with the default options. The MD5 hash of this QuiteRAT sample is 3d5747d4d5f363c986afc291c42d62cf.
Strike QuiteRAT_c027d641	This strike sends a malware sample known as QuiteRAT. QuiteRAT is composed of Qt libraries. It is believed to belong to the MagicRAT family and although made up of Qt does not have a GUI. QuiteRAT has been detected in a campaign utilizing CVE-2022-47966 to deploy the RAT. The MD5 hash of this QuiteRAT sample is c027d641c4c1e9d9ad048cda2af85db6.
Strike QuiteRAT_e969de0f	This strike sends a polymorphic malware sample known as QuiteRAT. QuiteRAT is composed of Qt libraries. It is believed to belong to the MagicRAT family and although made up of Qt does not have a GUI. QuiteRAT has been detected in a campaign utilizing CVE-2022-47966 to deploy the RAT. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this QuiteRAT sample is e969de0f656aed04259e4dc2a22bf55c.
Strike QuiteRAT_ec455ea2	This strike sends a polymorphic malware sample known as QuiteRAT. QuiteRAT is composed of Qt libraries. It is believed to belong to the MagicRAT family and although made up of Qt does not have a GUI. QuiteRAT has been detected in a campaign utilizing CVE-2022-47966 to deploy the RAT. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this QuiteRAT sample is ec455ea262331e229dacf88e5c36621b.
Strike QuiteRAT_f4e35caa	This strike sends a polymorphic malware sample known as QuiteRAT. QuiteRAT is composed of Qt libraries. It is believed to belong to the MagicRAT family and although made up of Qt does not have a GUI. QuiteRAT has been detected in a campaign utilizing CVE-2022-47966 to deploy the RAT. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this QuiteRAT sample is f4e35caab7658979002190faa27d009e.

<b>Name</b>	<b>Description</b>
Strike REvil_18786bfa	This strike sends a malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software was carried out against multiple MSPs and their customers. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The MD5 hash of this REvil sample is 18786bfac1be0ddf23ff94c029ca4d63.
Strike REvil_1a0545bb	This strike sends a polymorphic malware sample known as REvil. REvil malware also known as Sodinokibi operates as a ransomware-as-a-service (RaaS), that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this REvil sample is 1a0545bbcac7a44a1406cdac135288ca.
Strike REvil_2019e63a	This strike sends a polymorphic malware sample known as REvil. REvil malware also known as Sodinokibi operates as a ransomware-as-a-service (RaaS), that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The binary has been packed using upx packer, with the default options. The MD5 hash of this REvil sample is 2019e63a90b551b369bf42ede3827002.
Strike REvil_2075566e	This strike sends a malware sample known as REvil. REvil malware also known as Sodinokibi is a ransomware that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The MD5 hash of this REvil sample is 2075566e7855679d66705741dabe82b4.
Strike REvil_2c7ae560	This strike sends a polymorphic malware sample known as REvil. REvil malware also known as Sodinokibi is a ransomware that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this REvil sample is 2c7ae560e8df6f5c6d698edc2c860e83.
Strike REvil_31c17b36	This strike sends a polymorphic malware sample known as REvil. REvil malware also known as Sodinokibi is a ransomware that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The binary has been packed using upx packer, with the default options. The MD5 hash of this REvil sample is 31c17b36a1392448458c41447c040639.
Strike REvil_3777f3e0	This strike sends a malware sample known as REvil. REvil malware also known as Sodinokibi operates as a ransomware-as-a-service (RaaS), that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The MD5 hash of this REvil sample is 3777f3e092f2208c6670c01816562a7d.

<b>Name</b>	<b>Description</b>
Strike REvil_54079282	This strike sends a polymorphic malware sample known as REvil. REvil malware also known as Sodinokibi operates as a ransomware-as-a-service (RaaS), that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this REvil sample is 54079282596df0fff118c2cdf8c6cbe3.
Strike REvil_561cffba	This strike sends a malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software against multiple MSPs and their customers was reported. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The MD5 hash of this REvil sample is 561cffbab71a6e8cc1cdceda990ead4.
Strike REvil_585d9cf2	This strike sends a polymorphic malware sample known as REvil. REvil malware also known as Sodinokibi is a ransomware that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this REvil sample is 585d9cf2230ea8c331c911d1762db092.
Strike REvil_5d8bf296	This strike sends a polymorphic malware sample known as REvil. REvil malware also known as Sodinokibi is a ransomware that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this REvil sample is 5d8bf296740b5399e0d6a70a5585a557.
Strike REvil_63a945da	This strike sends a malware sample known as REvil. REvil malware also known as Sodinokibi operates as a ransomware-as-a-service (RaaS), that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The MD5 hash of this REvil sample is 63a945da1a63a8e56e8220c4ccf7fd0c.
Strike REvil_6e4e9299	This strike sends a polymorphic malware sample known as REvil. REvil malware also known as Sodinokibi is a ransomware that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The binary has random bytes appended at the end of the file. The MD5 hash of this REvil sample is 6e4e92997bbb44ee50a69ff1e6f61ba7.
Strike REvil_79668390	This strike sends a polymorphic malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software was carried out against multiple MSPs and their customers. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The binary has been packed using upx packer, with the default options. The MD5 hash of this REvil sample is 796683909b5036791e015a01609dc751.

<b>Name</b>	<b>Description</b>
Strike REvil_835f242d	This strike sends a malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software was carried out against multiple MSPs and their customers. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The MD5 hash of this REvil sample is 835f242dde220cc76ee5544119562268.
Strike REvil_8c26763d	This strike sends a polymorphic malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software was carried out against multiple MSPs and their customers. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this REvil sample is 8c26763d51dcec8d6683558e395b7f17.
Strike REvil_94d08716	This strike sends a malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software was carried out against multiple MSPs and their customers. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The MD5 hash of this REvil sample is 94d087166651c0020a9e6cc2fdacdc0c.
Strike REvil_95eb5380	This strike sends a malware sample known as REvil. REvil malware also known as Sodinokibi is a ransomware that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The MD5 hash of this REvil sample is 95eb5380f665c8f21795b5ef2716f86d.
Strike REvil_9ecc170	This strike sends a malware sample known as REvil. REvil malware also known as Sodinokibi operates as a ransomware-as-a-service (RaaS), that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The MD5 hash of this REvil sample is 9ecc170d0515fb14c8b78302b8053e7.
Strike REvil_a47cf00a	This strike sends a malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software was carried out against multiple MSPs and their customers. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The MD5 hash of this REvil sample is a47cf00aedf769d60d58bfe00c0b5421.
Strike REvil_ad49374e	This strike sends a malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software was carried out against multiple MSPs and their customers. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The MD5 hash of this REvil sample is ad49374e3c72613023fe420f0d6010d9.

<b>Name</b>	<b>Description</b>
Strike REvil_b26fbb99	This strike sends a polymorphic malware sample known as REvil. REvil malware also known as Sodinokibi operates as a ransomware-as-a-service (RaaS), that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The binary has random bytes appended at the end of the file. The MD5 hash of this REvil sample is b26fbb999449caad351b18364a17bd6e.
Strike REvil_b67606d3	This strike sends a malware sample known as REvil. REvil malware also known as Sodinokibi operates as a ransomware-as-a-service (RaaS), that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The MD5 hash of this REvil sample is b67606d382f50ebf76848d023deceee20.
Strike REvil_b7ba5484	This strike sends a malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software was carried out against multiple MSPs and their customers. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The MD5 hash of this REvil sample is b7ba5484a95ceec8374f49c21212853c.
Strike REvil_c3afcdff	This strike sends a malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software was carried out against multiple MSPs and their customers. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The MD5 hash of this REvil sample is c3afcdffa4aeeee56b80cf2fd3c9758c.
Strike REvil_cce629db	This strike sends a malware sample known as REvil. REvil malware also known as Sodinokibi operates as a ransomware-as-a-service (RaaS), that has recently been seen targeting law firms of A-list celebrities. The attackers not only pose the threat of losing all encrypted data but of also leaking stolen client data to the public. The MD5 hash of this REvil sample is cce629db2606ae98ba6e931adb1aeaee.
Strike REvil_ce1eefe4	This strike sends a polymorphic malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software was carried out against multiple MSPs and their customers. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this REvil sample is ce1eefe48010f4946cf45ffd6c4bebfa.
Strike REvil_eabb9030	This strike sends a polymorphic malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software against multiple MSPs and their customers was reported. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The binary has the timestamp field updated in the PE file header. The MD5 hash of this REvil sample is eabb90300cc0e02299681a93ad1db181.

<b>Name</b>	<b>Description</b>
Strike REvil_f31b13a0	This strike sends a polymorphic malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software was carried out against multiple MSPs and their customers. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this REvil sample is f31b13a0c700a35bc36376da03419df9.
Strike REvil_f6e2317b	This strike sends a polymorphic malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software against multiple MSPs and their customers was reported. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The binary has the checksum removed in the PE file format. The MD5 hash of this REvil sample is f6e2317b5ed7878efd7e1160b3bfc93d.
Strike REvil_f81958d7	This strike sends a polymorphic malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software against multiple MSPs and their customers was reported. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this REvil sample is f81958d74101253e7d1f14fe4c6ff560.
Strike REvil_fa4fb07b	This strike sends a polymorphic malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software was carried out against multiple MSPs and their customers. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this REvil sample is fa4fb07b8139347c27b5087b1ce4a524.
Strike REvil_ffedad13	This strike sends a polymorphic malware sample known as REvil. In July of 2021 a supply chain ransomware attack leveraging an SQL injection vulnerability in Kaseya VSA software was carried out against multiple MSPs and their customers. The ransomware being used in this attack, REvil also known as Sodinokibi, was pushed via an automated malicious update to their customers. The binary has the timestamp field updated in the PE file header. The MD5 hash of this REvil sample is ffedad13fdbd2cf0996cf728e8c1b4c11.
Strike Raccoon_283b0656	This strike sends a malware sample known as Raccoon. Raccoon stealer is a information-stealer. It exfiltrates various system information like installed applications, computer name, current user. It also steals cookies and autofill form details from various browsers. The MD5 hash of this Raccoon sample is 283b0656f28320fd0aa83a26824855cf.
Strike Raccoon_2d69a095	This strike sends a malware sample known as Raccoon. Raccoon stealer is a information-stealer. It exfiltrates various system information like installed applications, computer name, current user. It also steals cookies and autofill form details from various browsers. The MD5 hash of this Raccoon sample is 2d69a095559a07acef77116de389b272.

<b>Name</b>	<b>Description</b>
Strike Raccoon_53524af9	This strike sends a malware sample known as Raccoon. Raccoon stealer is a information-stealer. It exfiltrates various system information like installed applications, computer name, current user. It also steals cookies and autofill form details from various browsers. The MD5 hash of this Raccoon sample is 53524af959705823b05bd4b021d3e161.
Strike Raccoon_564d8629	This strike sends a malware sample known as Raccoon. Raccoon stealer is a information-stealer. It exfiltrates various system information like installed applications, computer name, current user. It also steals cookies and autofill form details from various browsers. The MD5 hash of this Raccoon sample is 564d8629438ee4bbe22f7ee0986ad7d7.
Strike Raccoon_a55b3026	This strike sends a malware sample known as Raccoon. Raccoon stealer is a information-stealer. It exfiltrates various system information like installed applications, computer name, current user. It also steals cookies and autofill form details from various browsers. The MD5 hash of this Raccoon sample is a55b3026f8a2acbb6c2efcbc6eeeef0b0.
Strike Raccoon_b230f688	This strike sends a malware sample known as Raccoon. Raccoon stealer is a information-stealer. It exfiltrates various system information like installed applications, computer name, current user. It also steals cookies and autofill form details from various browsers. The MD5 hash of this Raccoon sample is b230f68837746527efda1e032bc24aa2.
Strike Raccoon_c6ea6e2b	This strike sends a malware sample known as Raccoon. Raccoon stealer is a information-stealer. It exfiltrates various system information like installed applications, computer name, current user. It also steals cookies and autofill form details from various browsers. The MD5 hash of this Raccoon sample is c6ea6e2bafc9c176e2b8927b2d54f8b9.
Strike Raccoon_cf8ccc06	This strike sends a malware sample known as Raccoon. Raccoon stealer is a information-stealer. It exfiltrates various system information like installed applications, computer name, current user. It also steals cookies and autofill form details from various browsers. The MD5 hash of this Raccoon sample is cf8ccc063244e545ce6a04ec075d924b.
Strike Raccoon_d49de315	This strike sends a malware sample known as Raccoon. Raccoon stealer is a information-stealer. It exfiltrates various system information like installed applications, computer name, current user. It also steals cookies and autofill form details from various browsers. The MD5 hash of this Raccoon sample is d49de31596e0a19fe5e04ec96728014c.
Strike Raccoon_e90f9826	This strike sends a polymorphic malware sample known as Raccoon. Raccoon stealer is a information-stealer. It exfiltrates various system information like installed applications, computer name, current user. It also steals cookies and autofill form details from various browsers. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Raccoon sample is e90f98265063e09cad2d111be940e514.

<b>Name</b>	<b>Description</b>
Strike Rafel RAT_21c2de1e	This strike sends a malware sample known as Rafel RAT. Rafel RAT is an open-source Android based malware. It gives the attacker the ability to remotely control the infected Android device, enabling a range of malicious activities from data theft to device manipulation. The MD5 hash of this Rafel RAT sample is 21c2de1ee0ea905c3c9ed6ab1bb09ced.
Strike Rafel RAT_4e604e03	This strike sends a malware sample known as Rafel RAT. Rafel RAT is an open-source Android based malware. It gives the attacker the ability to remotely control the infected Android device, enabling a range of malicious activities from data theft to device manipulation. The MD5 hash of this Rafel RAT sample is 4e604e03cba3ad8da5f1ebbd7ba100bb.
Strike Rafel RAT_578ab3fb	This strike sends a malware sample known as Rafel RAT. Rafel RAT is an open-source Android based malware. It gives the attacker the ability to remotely control the infected Android device, enabling a range of malicious activities from data theft to device manipulation. The MD5 hash of this Rafel RAT sample is 578ab3fb6d1b6313f106518128053931.
Strike Rainyday_3b636a75	This strike sends a malware sample known as Rainyday. Rainyday is a backdoor malware that has been associated with the Firefly group. This malware has been tied to Chinese espionage groups that target telecom operators. The goal of this campaign and this malware is to steal credentials. The MD5 hash of this Rainyday sample is 3b636a75f3df29efcb6a602204f0a2a2.
Strike Rainyday_617469a8	This strike sends a malware sample known as Rainyday. Rainyday is a backdoor malware that has been associated with the Firefly group. This malware has been tied to Chinese espionage groups that target telecom operators. The goal of this campaign and this malware is to steal credentials. The MD5 hash of this Rainyday sample is 617469a87f5148913abf68536351f3a3.
Strike Rainyday_edada1b4	This strike sends a malware sample known as Rainyday. Rainyday is a backdoor malware that has been associated with the Firefly group. This malware has been tied to Chinese espionage groups that target telecom operators. The goal of this campaign and this malware is to steal credentials. The MD5 hash of this Rainyday sample is edada1b4d3393aab4ea96ad495817d12.
Strike Ramnit_015cf276	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as 'wallet', 'passwords', or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 015cf2765856e5eeb4c1b21f1782948f.
Strike Ramnit_01c0fdd0	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 01c0fdd09a4efe4c667021615d200281.

<b>Name</b>	<b>Description</b>
Strike Ramnit_033a8ac1	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has been packed using upx packer, with the default options. The MD5 hash of this Ramnit sample is 033a8ac18c77b06769416522d340c7d6.
Strike Ramnit_035fa9e4	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 035fa9e444203356d0823a23c516c6fa.
Strike Ramnit_04cbcba0	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 04cbcba0a0651a66cdcca68366862617.
Strike Ramnit_072ba4da	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 072ba4daab79f726d03cd3276339f31a.
Strike Ramnit_07a5a2e2	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 07a5a2e2114105d245de8bd46e67144e.
Strike Ramnit_0a48bae2	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 0a48bae2ff4780521936d8b94d3b0ce0.
Strike Ramnit_0cb76b7c	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 0cb76b7c17efe13b528796e2fecbb7f2.

<b>Name</b>	<b>Description</b>
Strike Ramnit_1094a6e5	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as 'wallet', 'passwords', or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 1094a6e574137656568228ffcd4f7d89.
Strike Ramnit_10c4d29b	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 10c4d29b442948f91cb8b507866db58e.
Strike Ramnit_123c4240	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 123c42409ca00eff4d535b31e6a13611.
Strike Ramnit_143ac294	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 143ac29473a7113ff66da39e65493583.
Strike Ramnit_1497c5fe	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 1497c5fe617e8f1ebba9eda07972dcd1.
Strike Ramnit_155b6238	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as 'wallet', 'passwords', or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 155b6238f6b847c8e95ee3c8fe6f7aa6.
Strike Ramnit_156ff7ed	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 156ff7ed174247ad7a7132fa51664949.

<b>Name</b>	<b>Description</b>
Strike Ramnit_19be3fa4	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 19be3fa4cdc9d2b92a71bd35dcd6c11a.
Strike Ramnit_1ba2b53f	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has the checksum removed in the PE file format. The MD5 hash of this Ramnit sample is 1ba2b53f4853d7f3f1c56dea3120a997.
Strike Ramnit_1da7901e	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 1da7901ed6ead6f61b598aaa01f3a563.
Strike Ramnit_1fdbd04b5	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 1fdbd04b583d20199bc27a8899ac6c533.
Strike Ramnit_21fb697b	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 21fb697b9475e8789e417c941f80fd36.
Strike Ramnit_29442acf	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 29442acf82ca85c78134021d6064d37.
Strike Ramnit_2a5133e9	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 2a5133e9c5a5a92cefaa4776ffe7ec18.

<b>Name</b>	<b>Description</b>
Strike Ramnit_2bef963c	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 2bef963c0d8b3c5d796dac3541489c08.
Strike Ramnit_2e6f8578	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Ramnit sample is 2e6f85784adb24f74ece54dab4400d1d.
Strike Ramnit_3123ff95	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 3123ff955e554c6ddfaaae2619fbf997.
Strike Ramnit_3538362a	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Ramnit sample is 3538362a5cb0dc951db93503999581d1.
Strike Ramnit_3703f175	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 3703f175acfc146e4269949a95dd5aa8.
Strike Ramnit_39cedb55	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 39cedb556b1eb185090954d43ffcfbd6.

<b>Name</b>	<b>Description</b>
Strike Ramnit_3eb1a18b	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 3eb1a18b4c1516e434c54d6ef8a151cc.
Strike Ramnit_46fa52f9	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 46fa52f9a733aac55c9fac0d53199d77.
Strike Ramnit_48142b72	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 48142b72881087b05a8c90d19fe60fba.
Strike Ramnit_489ed53d	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 489ed53d902055c17f31d98a71264ac4.
Strike Ramnit_490c6d87	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 490c6d879fc151b65dfab998df0fbc37.
Strike Ramnit_4a7a546c	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 4a7a546c94e0918c95ae5a4cc9575042.
Strike Ramnit_4f5e5502	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 4f5e5502685c22b184d3069621e4df93.

<b>Name</b>	<b>Description</b>
Strike Ramnit_503873bc	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as 'wallet', 'passwords', or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Ramnit sample is 503873bce18b69191ecc713fe84b5861.
Strike Ramnit_520c2909	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 520c2909c35be0ed73fa17fc56f43aa4.
Strike Ramnit_52efe8c8	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 52efe8c8b4205a6c099ade4e32aeea32.
Strike Ramnit_55ff5d7e	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 55ff5d7e137dd97103613126e086b026.
Strike Ramnit_58eeb6a2	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 58eeb6a25c267ee5121a1fa8c5b06737.
Strike Ramnit_5cce25c0	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 5cce25c024adfe8fddd9d6261ea76f55.
Strike Ramnit_5e135573	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 5e13557300fce99cd3f4176946f55461.

<b>Name</b>	<b>Description</b>
Strike Ramnit_5f93cc93	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 5f93cc93468bc848f78e9e643a3e8607.
Strike Ramnit_6414f5d9	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 6414f5d9c9599094e4c28f5a2814cf76.
Strike Ramnit_64823e3a	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 64823e3ac192f97854cbecc718b7812e.
Strike Ramnit_68464084	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 68464084c82fdbd09faebcbf040dfc7c4.
Strike Ramnit_6b829c72	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as 'wallet', 'passwords', or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 6b829c727cb7a49186d314d7a92e8836.
Strike Ramnit_72acc4b7	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 72acc4b7e3fba55ed74b0f9a4defad94.
Strike Ramnit_72fc20bc	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has random bytes appended at the end of the file. The MD5 hash of this Ramnit sample is 72fc20bc09671f90a18adf847fac8b9d.

<b>Name</b>	<b>Description</b>
Strike Ramnit_7bbe1db6	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 7bbe1db690fcd36ae9801c66034bb326.
Strike Ramnit_7c3272f7	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 7c3272f758022b290adddbab3710823a.
Strike Ramnit_7e4bbf1b	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 7e4bbf1bb97b22f8e034a488cc44d7dd.
Strike Ramnit_80d7449c	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 80d7449c3200c92e5018a8c6d83125a3.
Strike Ramnit_874f6bbf	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 874f6bbfd5a21b95ff267b4be07b1f83.
Strike Ramnit_8a70a1fc	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 8a70a1fc4e7bbd01f9b16d272692eed7.
Strike Ramnit_8ab7b9dc	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Ramnit sample is 8ab7b9dc6d79d080f9a31bd29ca728a7.

<b>Name</b>	<b>Description</b>
Strike Ramnit_8accfce0	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as 'wallet', 'passwords', or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 8accfce046866ad405d30b235d1e5205.
Strike Ramnit_932314df	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 932314dfc7c4f74f1ab12d906964874e.
Strike Ramnit_950b594c	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 950b594ce028b271ccecb184aa895bb3.
Strike Ramnit_959c6743	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 959c67436d11558210e610bf14d9d04b.
Strike Ramnit_96b5e6be	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 96b5e6be621a0dd3d889a7c43342a4f7.
Strike Ramnit_97fdbb3c	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is 97fdbb3c51dc510b5f5a18310deabaf3.
Strike Ramnit_a43b1f59	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as 'wallet', 'passwords', or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is a43b1f59decbcaa066b65e4e83f644ed.

<b>Name</b>	<b>Description</b>
Strike Ramnit_a58cd8d6	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as 'wallet', 'passwords', or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Ramnit sample is a58cd8d6d609509f29fc64d8d559f8a7.
Strike Ramnit_a836be5e	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Ramnit sample is a836be5e19a62d1ffd8f41b15ded88a0.
Strike Ramnit_a86bc086	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is a86bc0861253da313629974ddfdfafaa.
Strike Ramnit_a87f228d	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has random bytes appended at the end of the file. The MD5 hash of this Ramnit sample is a87f228d3bc2b4209b50d101910d55cd.
Strike Ramnit_abb242e9	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is abb242e98dd7d6971cdfa83d9f448e0e.
Strike Ramnit_abe7f205	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is abe7f2053560567b363508fb0a8a3501.

<b>Name</b>	<b>Description</b>
Strike Ramnit_acb95321	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is acb95321ac7ff2b0ea2ca2519e376113.
Strike Ramnit_b01a35f1	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is b01a35f1ccd89837036a68172bb57d03.
Strike Ramnit_b0a9e215	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is b0a9e215276bfe98a7df9cf2d771326e.
Strike Ramnit_b3632d95	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is b3632d958616bac3b775d19f3347f6cd.
Strike Ramnit_b3be362c	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Ramnit sample is b3be362cd54d0bc8d6c75495ec769aa5.
Strike Ramnit_b45db996	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is b45db99697ceede9ff6d47b0c1bcb7c6.
Strike Ramnit_b4a403f5	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is b4a403f53da0d72524dd7600b7d68dca.

<b>Name</b>	<b>Description</b>
Strike Ramnit_b79e36ca	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is b79e36ca7388fc38cb764cf807790645.
Strike Ramnit_b88a349e	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is b88a349e3e1bbb289a66deaf3bd053fb.
Strike Ramnit_b9ebd609	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as 'wallet', 'passwords', or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is b9ebd609a6bdb6ffcce8067631cc6a05.
Strike Ramnit_bbb2d2c7	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is bbb2d2c7a02bb20e476ef9ea2483d575.
Strike Ramnit_bc3251e5	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as 'wallet', 'passwords', or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is bc3251e5b02d7ba902c7f80001189e78.
Strike Ramnit_bf70c723	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is bf70c7230fb57e3732a87cc5b09defa3.
Strike Ramnit_c343691e	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Ramnit sample is c343691e1d43b9ddc5a22d374937f4e6.

<b>Name</b>	<b>Description</b>
Strike Ramnit_c5e9c5a8	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is c5e9c5a84aa05ff1d389d5ed0d4d97d6.
Strike Ramnit_c6d47278	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is c6d472784b73e47ea8af9f50ce45fb58.
Strike Ramnit_c9c78028	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is c9c7802846ec211aa5b59cccd60e2bb26.
Strike Ramnit_ca5003a7	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as 'wallet', 'passwords', or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is ca5003a7e45e2962b2c2a40fd250480e.
Strike Ramnit_ca7fa159	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has the checksum removed in the PE file format. The MD5 hash of this Ramnit sample is ca7fa159e398a1f921e4453db3df0f51.
Strike Ramnit_ccbf0c65	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is ccbf0c6561f9f4cbd092bccab0455734.
Strike Ramnit_cf59b414	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is cf59b414c4fcc1618f5e7d10f74a442f.

<b>Name</b>	<b>Description</b>
Strike Ramnit_cf99487a	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is cf99487abb258b230c1ff2b484a6161a.
Strike Ramnit_d2d4536a	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is d2d4536a287c967104dec2d4a3fb7e3b.
Strike Ramnit_d3185fb0	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has a new section added in the PE file format with random contents. The MD5 hash of this Ramnit sample is d3185fb0ca81273a1274ae564ab59436.
Strike Ramnit_d475fd84	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is d475fd848f01340ad4219ff55b6bc52e.
Strike Ramnit_d483d877	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Ramnit sample is d483d877023f757c74a9f555a5f4389e.
Strike Ramnit_d59c82a0	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is d59c82a0ed4995f10218a4bd21d3d34a.

<b>Name</b>	<b>Description</b>
Strike Ramnit_d88b7c70	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is d88b7c7005b6159d6cef5c6f2c19b8a6.
Strike Ramnit_dc856ff4	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary file has one more imports added in the import table. The MD5 hash of this Ramnit sample is dc856ff4eb38952dff21462a433856f.
Strike Ramnit_dcc2ef65	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is dcc2ef65093337449166f3f0fd3cd3be.
Strike Ramnit_dd94d5eb	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is dd94d5eb41eaa2a1c73ad981b08a7f1a.
Strike Ramnit_dfec76cc	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as 'wallet', 'passwords', or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is dfec76ccb2fdc6de5cbf221f027e5493.
Strike Ramnit_e00b89ed	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is e00b89ed3e888871c868c9551c670eb2.
Strike Ramnit_e0e03149	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is e0e031498e3199f6d7927282f6b97c10.

<b>Name</b>	<b>Description</b>
Strike Ramnit_e26a0a6b	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is e26a0a6b399f76d05026ac01949bed83.
Strike Ramnit_e5c576c9	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is e5c576c9eae8d572b7c52a869a9dfeec.
Strike Ramnit_ecd995eb	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is ecd995ebc8f0278728cd44682da5bcd.
Strike Ramnit_ed3b2b9c	This strike sends a polymorphic malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Ramnit sample is ed3b2b9c4229f012d320f6ccee318ce9.
Strike Ramnit_ef24a361	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is ef24a361def1b7142a346afbcda9aafd.
Strike Ramnit_f123c76c	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is f123c76c8591b80f17fb87c68ff768cf.
Strike Ramnit_f2e58f4e	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as 'wallet', 'passwords', or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is f2e58f4eaa5a900dc3af4d152b0cdb50.

<b>Name</b>	<b>Description</b>
Strike Ramnit_f457f41a	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is f457f41a6bd5a0a1e4608c8a097d6a43.
Strike Ramnit_f8224fd6	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is f8224fd6a29b1ca1258840c26cddaab3.
Strike Ramnit_f874de55	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is f874de5541c3e154c13c0c9a5fe9797d.
Strike Ramnit_fc3a1beb	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is fc3a1beb19c6cd9bce76ea8120589519.
Strike Ramnit_feb53bd5	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as wallet, passwords or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is feb53bd59761634c646bc71f060b22b0.
Strike Ramnit_ff850214	This strike sends a malware sample known as Ramnit. Ramnit is a banking trojan that has been around since 2010 and has recently been resuming activity. After infection, it scans files that have interesting keywords, such as "wallet", "passwords", or the names of the targeted banks. Ramnit uses malvertising and malware-laden spam for distribution, though it also employed popular exploit kits, such as Angler. The MD5 hash of this Ramnit sample is ff8502146514a7a68a0cf0e62c72feb.

<b>Name</b>	<b>Description</b>
Strike RapperBot_1318afe2	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 1318afe218cf3a86f71aa6936df33ee7.
Strike RapperBot_1bdfcca7	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 1bdfcca7b35ad31a41fba5d6dc88b276.
Strike RapperBot_2e974038	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 2e9740382e75ebb7c8f4a0cdf2c36500.
Strike RapperBot_30ce66fa	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 30ce66fa45abddf278dbb3eccf87ddad.
Strike RapperBot_46da0686	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 46da0686e0ad65ee44f4cac5f6558ec9.

<b>Name</b>	<b>Description</b>
Strike RapperBot_5630ee34	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 5630ee34393ce22d317c3a11a91b5bb2.
Strike RapperBot_5a2fe024	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 5a2fe024029c7b8894885ded5f08e42e.
Strike RapperBot_5ab947f7	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 5ab947f7cae22fa65398c591e1aed268.
Strike RapperBot_5d7d2618	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 5d7d2618e09ea3c84f5a484553e0ea65.
Strike RapperBot_5e10e46c	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 5e10e46cccd75627df169976de506029d.

<b>Name</b>	<b>Description</b>
Strike RapperBot_64e0ddc2	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 64e0ddc2aa51350b355434ffd1a4d6b6.
Strike RapperBot_669a8e06	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 669a8e0683154f594a110d129d96a068.
Strike RapperBot_6faeac8f	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 6faeac8f2269c3d86606b34de90607fd.
Strike RapperBot_72c70d37	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 72c70d37a714ecf026cdea998c36a069.
Strike RapperBot_75181839	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 75181839d4eca01c095f5976cfe06f71.

<b>Name</b>	<b>Description</b>
Strike RapperBot_927b2162	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 927b2162032a3a89a6e17f9769155985.
Strike RapperBot_94c9ae3a	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 94c9ae3ab4319954a302d819e8a608ec.
Strike RapperBot_9d8cd6a7	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is 9d8cd6a75e40c2022abca1e58c88b40f.
Strike RapperBot_ab96e594	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is ab96e594403ed957ed2ec6c992513abf.
Strike RapperBot_bda8d5c2	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is bda8d5c2665f47877ab571728f07c65a.

<b>Name</b>	<b>Description</b>
Strike RapperBot_ce1a9802	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is ce1a980265811fd257b36a449b987702.
Strike RapperBot_e4b3a9f9	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is e4b3a9f9e5e90ce3912665ff7e0f6f8.
Strike RapperBot_e70f70c9	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is e70f70c91670ac3fc8d3d7963f6fb8a6.
Strike RapperBot_e94c6fa4	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is e94c6fa46fb3ad76973a221fa75c9557.
Strike RapperBot_ee73067c	This strike sends a malware sample known as RapperBot. RapperBot is an IoT botnet malware that heavily borrows from Mirai source code. However, unlike Mirai, RapperBot brute forces vulnerable SSH servers. Upon successfully breaking into the SSH server, the credentials are sent back to the command-and-control server, and then the malware adds its public key to the authorized keys file in an attempt to maintain persistence on the machine. This primes the malware for future DDoS attacks on the target when the attackers are ready. The MD5 hash of this RapperBot sample is ee73067c97e7015dc3f805fd3f66f3db.
Strike Razy_0115c1e9	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 0115c1e94464d6c03da80b814af18146.

<b>Name</b>	<b>Description</b>
Strike Razy_0206fb01	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 0206fb018cf06a3876e7694ccae14151.
Strike Razy_090fc943	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 090fc94335cead75e2888a74f810cf61.
Strike Razy_0c56c0cf	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 0c56c0cf7ddb488dce5757499b0a5504.
Strike Razy_0dd8ba9e	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 0dd8ba9e4af52d8cfcd1f12b856f44060.
Strike Razy_0f171259	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 0f1712592ba72483bbf0dd935b643191.
Strike Razy_0ff887b5	This strike sends a polymorphic malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Razy sample is 0ff887b5bb3bd7d397e5a185f60d3110.
Strike Razy_1e12692a	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 1e12692a237866f2f8df7d5f16444752.
Strike Razy_201dd9a3	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 201dd9a3dac6d9fc554914615c5944ad.
Strike Razy_22f324e1	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 22f324e17259132c9b849a25159b18ad.
Strike Razy_23e05fe4	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 23e05fe438c220ff0b393133a5cd0865.

<b>Name</b>	<b>Description</b>
Strike Razy_252b278e	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 252b278eca0767c82901c901c3cf469.
Strike Razy_2545d1f5	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 2545d1f5a918407da1518fb6b190c8a4.
Strike Razy_2b1b280b	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 2b1b280b058d852abf280b590b6b4a6d.
Strike Razy_2dfcb53d	This strike sends a polymorphic malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Razy sample is 2dfcb53dc629952fe13243ce4065e2c1.
Strike Razy_2ea5d78a	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 2ea5d78aab51ab807a91a44d5b76f1d5.
Strike Razy_2f600beb	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 2f600bebf301bb078c8e27505c37cf31.
Strike Razy_2f7483ba	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 2f7483ba3742b150b83cf1f643a6b6d7.
Strike Razy_2f86beaa	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 2f86beaab3b9b487047581b6be68fd6b.
Strike Razy_3a3b7b73	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 3a3b7b73c496357f2ff33b3b821d1330.
Strike Razy_3b0e0563	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 3b0e0563d8e5d58dab416cef38ca179c.

<b>Name</b>	<b>Description</b>
Strike Razy_3fb806a5	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 3fb806a542e7b8105a423541357c4b8b.
Strike Razy_408a2d09	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 408a2d09fddf9ba44cac548bb77173a7.
Strike Razy_42570f5d	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 42570f5dd072311421769b660b8d3b23.
Strike Razy_47edd917	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 47edd917ab49602626cf46c6781c87e.
Strike Razy_48693a04	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 48693a04e8279cf484232ddda0373eb.
Strike Razy_4d70c597	This strike sends a polymorphic malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Razy sample is 4d70c59732528de1e9989715969b27cd.
Strike Razy_534f0c05	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 534f0c051bb0d2a53e6c1e0998431281.
Strike Razy_53ad5cd4	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 53ad5cd4141a2ac1b9ac77e5b0f28eef.
Strike Razy_5d25dc38	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 5d25dc38a80f4a2bf96e40fc912c683a.
Strike Razy_5d412f49	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 5d412f493bf3599382b93dae9d321197.

<b>Name</b>	<b>Description</b>
Strike Razy_614a7da1	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 614a7da1251aea20e234b2024fd082f6.
Strike Razy_6e668a86	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 6e668a860579dbd302a187a98076b93a.
Strike Razy_77b5096d	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 77b5096d8ae7e182bf8a36d2349a64e0.
Strike Razy_77d8eca1	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 77d8eca1b5391ceb71c3317a5e6b6118.
Strike Razy_7b0ebe83	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 7b0ebe8345df9f422d2401fcc8e17832.
Strike Razy_7bdfb61d	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 7bdfb61dfb48061bb799543090f8bb54.
Strike Razy_7ee9e970	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 7ee9e9701b2c5d1b0345eea51fe0f564.
Strike Razy_8115eaff	This strike sends a polymorphic malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Razy sample is 8115eafffd3dc5616b473a855a1462a7.
Strike Razy_844d99c7	This strike sends a polymorphic malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The binary has random bytes appended at the end of the file. The MD5 hash of this Razy sample is 844d99c7d6902f04c4f2c834cc2d356b.
Strike Razy_89731bbf	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 89731bbf0ff24e5ab793221aa5fa793d.

<b>Name</b>	<b>Description</b>
Strike Razy_8d261a3f	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 8d261a3fbccb88a55798ceb0d95c558.
Strike Razy_8e765624	This strike sends a polymorphic malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Razy sample is 8e765624f020df424a152dab988a9723.
Strike Razy_967d450c	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 967d450cda75fadcb84009f55723311d0.
Strike Razy_9b6a7a52	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 9b6a7a5208bbb45777920653c8b23855.
Strike Razy_9bfd7e8	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 9bfd7e8a74bf91ea9d1a30d3f00e7aa.
Strike Razy_9ef22e9c	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is 9ef22e9c85adf31eff472e50319aa8bd.
Strike Razy_af9a9a77	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is af9a9a779a445b6ce83ff48adb53611d.
Strike Razy_b1d1bedb	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is b1d1bedb59a544bfa5beba3067560a1b.
Strike Razy_b42a8425	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is b42a842553913cbac45effdc053e9696.
Strike Razy_b99915c7	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is b99915c7b410a6460dd0f1e0281ee0be.

<b>Name</b>	<b>Description</b>
Strike Razy_b9a11c5d	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is b9a11c5d2dc977651fc892b50a18cc2d.
Strike Razy_b9bde5f9	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is b9bde5f9ae8e82d14e7e2edab02885a6.
Strike Razy_bb99864d	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is bb99864d4aef505915898a5b42db891b.
Strike Razy_bc68cf1c	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is bc68cf1cb8bc229686ef89a93b6a12fa.
Strike Razy_c9f10d7c	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is c9f10d7c9f46eacb6dce566f889fa8b1.
Strike Razy_cae50e27	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is cae50e27b70d5bab0e7b7ee5ddbaae89.
Strike Razy_d1438e27	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is d1438e27f636d45aa5ad7fd64ca3a340.
Strike Razy_dd965327	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is dd965327fe9900628f84aabaf4ee34e.
Strike Razy_e609a6c2	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is e609a6c2c348dc5e0ca3b7b4d62b6883.
Strike Razy_e8040f28	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is e8040f28bb69b4253d3b26b058a9f8ce.

<b>Name</b>	<b>Description</b>
Strike Razy_f1c1283d	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is f1c1283d8cac50b7b8e9c0541f254d08.
Strike Razy_f62eb7cd	This strike sends a polymorphic malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Razy sample is f62eb7cdd299f57a2a54961e8479a56a.
Strike Razy_f6be4584	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is f6be458489923d7fa91bf8d6f28aa5af.
Strike Razy_f93a2a58	This strike sends a polymorphic malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The binary has random bytes appended at the end of the file. The MD5 hash of this Razy sample is f93a2a5865439f6a08c183969e4e661e.
Strike Razy_faffdf7c	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is afffdf7c523de20379785fdbbef179f0.
Strike Razy_fcd67c80	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is fcd67c8088b3a39fab73c9cb47a86713.
Strike Razy_fd0902cb	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is fd0902cbf4bb6ba396f504965a663872.
Strike Razy_ffa27508	This strike sends a malware sample known as Razy. Razy is often used as a generic detection name for a Windows Trojan. This cluster of samples contains encrypted code in the resources section that could be injected to a legitimate process. The MD5 hash of this Razy sample is ffa275089b4a1ea0259f4343ac1f3c11.
Strike RedDriver_072ba230	This strike sends a malware sample known as RedDriver. RedDriver is a driver based web browser hijacker, that intercepts browser traffic with the Windows WFP. The MD5 hash of this RedDriver sample is 072ba2309b825ce1dba37d8d924ea8ed.
Strike RedDriver_1002bd73	This strike sends a malware sample known as RedDriver. RedDriver is a driver based web browser hijacker, that intercepts browser traffic with the Windows WFP. The MD5 hash of this RedDriver sample is 1002bd7325b7f739c004400808fb5888.

<b>Name</b>	<b>Description</b>
Strike RedDriver_15d9504f	This strike sends a malware sample known as RedDriver. RedDriver is a driver based web browser hijacker, that intercepts browser traffic with the Windows WFP. The MD5 hash of this RedDriver sample is 15d9504fec29a115c5bd86c22ce3d096.
Strike RedDriver_27ff3ec8	This strike sends a malware sample known as RedDriver. RedDriver is a driver based web browser hijacker, that intercepts browser traffic with the Windows WFP. The MD5 hash of this RedDriver sample is 27ff3ec8ae8931c3a500b2a44d3afa45.
Strike RedDriver_381c48ba	This strike sends a malware sample known as RedDriver. RedDriver is a driver based web browser hijacker, that intercepts browser traffic with the Windows WFP. The MD5 hash of this RedDriver sample is 381c48ba28b806dad43e9d363e639ef6.
Strike RedDriver_5aeab942	This strike sends a malware sample known as RedDriver. RedDriver is a driver based web browser hijacker, that intercepts browser traffic with the Windows WFP. The MD5 hash of this RedDriver sample is 5aeab9427d85951def146b4c0a44fc63.
Strike RedDriver_adb8e404	This strike sends a malware sample known as RedDriver. RedDriver is a driver based web browser hijacker, that intercepts browser traffic with the Windows WFP. The MD5 hash of this RedDriver sample is adb8e404ae0dcfd2d937dbe6f7dbc6d77.
Strike RedDriver_d209d42e	This strike sends a malware sample known as RedDriver. RedDriver is a driver based web browser hijacker, that intercepts browser traffic with the Windows WFP. The MD5 hash of this RedDriver sample is d209d42e2d604e6018129634fc2a2f38.
Strike RedDriver_e026b266	This strike sends a malware sample known as RedDriver. RedDriver is a driver based web browser hijacker, that intercepts browser traffic with the Windows WFP. The MD5 hash of this RedDriver sample is e026b2666d2ae5583a934b0f9d4b5d03.
Strike RedDriver_e7c1a57c	This strike sends a malware sample known as RedDriver. RedDriver is a driver based web browser hijacker, that intercepts browser traffic with the Windows WFP. The MD5 hash of this RedDriver sample is e7c1a57c2a8dd073b45974719459c2ee.
Strike RedGoBot_0c817d83	This strike sends a malware sample known as RedGoBot. RedGoBot malware has recently been distributed in the wild via the exploitation of CVE 2021-35394. This malware is a DDoS botnet with the ability to execute remote commands on the operating system, terminate the bot client, and execute DDoS attacks on HTTP, ICMP, TCP, UDP, VSE, and OpenVPN protocols. The MD5 hash of this RedGoBot sample is 0c817d839e014ceb4350e6989ac85b08.
Strike RedGoBot_31be883a	This strike sends a malware sample known as RedGoBot. RedGoBot malware has recently been distributed in the wild via the exploitation of CVE 2021-35394. This malware is a DDoS botnet with the ability to execute remote commands on the operating system, terminate the bot client, and execute DDoS attacks on HTTP, ICMP, TCP, UDP, VSE, and OpenVPN protocols. The MD5 hash of this RedGoBot sample is 31be883a1346f656df5061bc784060a7.

<b>Name</b>	<b>Description</b>
Strike RedGoBot_3c404053	This strike sends a malware sample known as RedGoBot. RedGoBot malware has recently been distributed in the wild via the exploitation of CVE 2021-35394. This malware is a DDoS botnet with the ability to execute remote commands on the operating system, terminate the bot client, and execute DDoS attacks on HTTP, ICMP, TCP, UDP, VSE, and OpenVPN protocols. The MD5 hash of this RedGoBot sample is 3c404053296efd41dae11a0a39be3808.
Strike RedGoBot_75ade86d	This strike sends a malware sample known as RedGoBot. RedGoBot malware has recently been distributed in the wild via the exploitation of CVE 2021-35394. This malware is a DDoS botnet with the ability to execute remote commands on the operating system, terminate the bot client, and execute DDoS attacks on HTTP, ICMP, TCP, UDP, VSE, and OpenVPN protocols. The MD5 hash of this RedGoBot sample is 75ade86d5cb702c76576c587c167c451.
Strike RedGoBot_9dcc0ab0	This strike sends a malware sample known as RedGoBot. RedGoBot malware has recently been distributed in the wild via the exploitation of CVE 2021-35394. This malware is a DDoS botnet with the ability to execute remote commands on the operating system, terminate the bot client, and execute DDoS attacks on HTTP, ICMP, TCP, UDP, VSE, and OpenVPN protocols. The MD5 hash of this RedGoBot sample is 9dcc0ab0ecc5ece11a70d465dcd9b56b.
Strike RedGoBot_aaee43e6	This strike sends a malware sample known as RedGoBot. RedGoBot malware has recently been distributed in the wild via the exploitation of CVE 2021-35394. This malware is a DDoS botnet with the ability to execute remote commands on the operating system, terminate the bot client, and execute DDoS attacks on HTTP, ICMP, TCP, UDP, VSE, and OpenVPN protocols. The MD5 hash of this RedGoBot sample is aaee43e63d5a3abd70ffa774a16c816e.
Strike RedGoBot_c1492f71	This strike sends a malware sample known as RedGoBot. RedGoBot malware has recently been distributed in the wild via the exploitation of CVE 2021-35394. This malware is a DDoS botnet with the ability to execute remote commands on the operating system, terminate the bot client, and execute DDoS attacks on HTTP, ICMP, TCP, UDP, VSE, and OpenVPN protocols. The MD5 hash of this RedGoBot sample is c1492f719a4553bb4280b5a8c8c39095.
Strike RedGoBot_cd56bea3	This strike sends a malware sample known as RedGoBot. RedGoBot malware has recently been distributed in the wild via the exploitation of CVE 2021-35394. This malware is a DDoS botnet with the ability to execute remote commands on the operating system, terminate the bot client, and execute DDoS attacks on HTTP, ICMP, TCP, UDP, VSE, and OpenVPN protocols. The MD5 hash of this RedGoBot sample is cd56bea395c994290ebc71cc1482dfe0.
Strike RedGoBot_fad7f107	This strike sends a malware sample known as RedGoBot. RedGoBot malware has recently been distributed in the wild via the exploitation of CVE 2021-35394. This malware is a DDoS botnet with the ability to execute remote commands on the operating system, terminate the bot client, and execute DDoS attacks on HTTP, ICMP, TCP, UDP, VSE, and OpenVPN protocols. The MD5 hash of this RedGoBot sample is fad7f1073fe267fca24927b626afaa1f.
Strike RedGoBot_fd1facf3	This strike sends a malware sample known as RedGoBot. RedGoBot malware has recently been distributed in the wild via the exploitation of CVE 2021-35394. This malware is a DDoS botnet with the ability to execute remote commands on the operating system, terminate the bot client, and execute DDoS attacks on HTTP, ICMP, TCP, UDP, VSE, and OpenVPN protocols. The MD5 hash of this RedGoBot sample is fd1facf3a3fcfa0fd6108bbbe98f8d5fd.

<b>Name</b>	<b>Description</b>
Strike Redline_208b1854	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 208b18547a5e4eca91494fd6ba71efd7.
Strike Redline_252fd129	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 252fd12929535d1f2dfffc12d7193c021.
Strike Redline_27bc5938	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 27bc593827f61fed5736d0c7f45d22c9.
Strike Redline_2b1f7a81	This strike sends a polymorphic malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 2b1f7a81e07e62474484cb4d97aa17f4.
Strike Redline_2ba90083	This strike sends a polymorphic malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 2ba900830e12d7101f23ccfd40d7f35f.
Strike Redline_3665532a	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 3665532a33daae6c4f5e114934c865ff.
Strike Redline_42726d38	This strike sends a polymorphic malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 42726d389d754a68a19bfedef69b2de2.
Strike Redline_4a7186b7	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 4a7186b73bb3dfa1ee69a25d2a6ad958.
Strike Redline_547196d7	This strike sends a polymorphic malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 547196d7ed538209379d8dd4e1c469ee.
Strike Redline_55fcdb39	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 55fcdb39dca31049eb2fe68fb4daad64.
Strike Redline_5726a848	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 5726a848ba4a8ca552c1ad8b9118d1b3.

<b>Name</b>	<b>Description</b>
Strike Redline_6097a5db	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 6097a5db8c5cab3c031969fabeea6244.
Strike Redline_73442058	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 73442058511cf24505d16d0e4739d248.
Strike Redline_78104cfcd	This strike sends a polymorphic malware sample known as Redline. Redline is an information-stealer malware written in .The binary has random contents appended in one of the existing sections in the PE file format.NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 78104cfdfa3117cfdafb40f67a925f54.
Strike Redline_81c788db	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 81c788db54fb65827f8317dba281351c.
Strike Redline_8ed60c6e	This strike sends a polymorphic malware sample known as Redline. Redline is an information-stealer malware written in .The binary has the debug flag removed in the PE file format.NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 8ed60c6e47675061036ddc314ed0fc1c.
Strike Redline_945955bb	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 945955bb867fb99aa6b2b2eed03840b5.
Strike Redline_99ee87c2	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 99ee87c2debc6a598b30622e35f19046.
Strike Redline_9ae9ad81	This strike sends a polymorphic malware sample known as Redline. Redline is an information-stealer malware written in .The binary has been packed using upx packer, with the default options.NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 9ae9ad81c4c0062130d7568a8f93ffd0.
Strike Redline_9c07bc1e	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 9c07bc1e99a6083c29dc32c8c84dff4a.
Strike Redline_9e266ed0	This strike sends a polymorphic malware sample known as Redline. Redline is an information-stealer malware written in .The binary has a random section name renamed according to the PE format specification.NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is 9e266ed096370c8c63276b949cd79232.
Strike Redline_a396d712	This strike sends a polymorphic malware sample known as Redline. Redline is an information-stealer malware written in .The binary has random strings (lorem ipsum) appended at the end of the file.NET, and it can be purchased on hacking forums The MD5 hash of this Redline sample is a396d712ef77c30f53b6299bfe4a28d3.

<b>Name</b>	<b>Description</b>
Strike Redline_a4358594	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is a43585940b7a2bb9f0af4587dc4fa1d4.
Strike Redline_b0ab5154	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is b0ab5154bb8b4ff883500f410342d580.
Strike Redline_b2ade0c7	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is b2ade0c7bdc22a3186cdb2d74aae89d7.
Strike Redline_b2f54c6a	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is b2f54c6a518bfbd5c1a4f075ff211b15.
Strike Redline_b619847a	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is b619847a7c65a0947cf7a132e510030d.
Strike Redline_c1828a78	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is c1828a782fe78675119058eea22fdbc2.
Strike Redline_c46105a3	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is c46105a343ef37ca940d93a01f465933.
Strike Redline_c7c0a75d	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is c7c0a75da9042c5b0a9d82e09fec7aa7.
Strike Redline_cf0b0970	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is cf0b097016e80ad6f9b8a9cf90d9d496.
Strike Redline_d1f9d682	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is d1f9d68214b2cf9f6a59891514b37e8f.
Strike Redline_d78c6b9a	This strike sends a polymorphic malware sample known as Redline. Redline is an information-stealer malware written in .NET. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Redline sample is d78c6b9a87cc61d7253a1b9fb8cb3669.
Strike Redline_d8e51ae2	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is d8e51ae2875cb0328b492c8238d4d1e0.

<b>Name</b>	<b>Description</b>
Strike Redline_e0856fc6	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is e0856fc6e4fa8144ff5b20a2fa16169f.
Strike Redline_e910b20c	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is e910b20cdae914ecd558f493e4df6a4f.
Strike Redline_ea49bd1b	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is ea49bd1b6b5a19618dff479ee0d2aa24.
Strike Redline_ee4fe7b4	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is ee4fe7b49973d4c3297aa4296a55b3b2.
Strike Redline_ef29de5f	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is ef29de5f57bf968677023aacb1faaf15.
Strike Redline_ef591ff4	This strike sends a polymorphic malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is ef591ff4904834fc43ecb3fb1a3519b6.
Strike Redline_f7271f16	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is f7271f1652341aee16bd3910c795b98a.
Strike Redline_fa34b83c	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is fa34b83c83f33e1bcc6c0ccaeb77172e.
Strike Redline_fd0e02dc	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is fd0e02dc2e477d0229807f2486fff6b8.
Strike Redline_fe13bef0	This strike sends a malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is fe13bef02933d061609d3f614bc0f303.
Strike Redline_fe574fcf	This strike sends a polymorphic malware sample known as Redline. Redline is an information-stealer malware written in .NET, and it can be purchased on hacking forums. The MD5 hash of this Redline sample is fe574fcf72faa87d2d786f8cf49eaadf.

<b>Name</b>	<b>Description</b>
Strike RemcosRAT_085d3471	This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is 085d3471e880c5f53fd98df14ccc23e7.
Strike RemcosRAT_0adde8b5	This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is 0adde8b59fdacd77b8030d1d7ab5431c.
Strike RemcosRAT_145349bb	This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is 145349bbf829a5f9276096963902e4ce.
Strike RemcosRAT_239898c6	This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is 239898c682bcb7091aaa57cd6d70f736.
Strike RemcosRAT_2bb1ea8	This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is 2bb1ea8d55eb6bb5607065a241622a2.

<b>Name</b>	<b>Description</b>
Strike RemcosRAT_3e1a5431	This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is 3e1a54314b67d65e343d7ded3466f8c1.
Strike RemcosRAT_4b724c9c	This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is 4b724c9c3ce7abc1612f4f811a01ca96.
Strike RemcosRAT_545111a0	This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is 545111a072d3fad3cf8964e1f0c9ae00.
Strike RemcosRAT_6ae9e6b7	This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is 6ae9e6b744b2779965c89e3bebcef94.
Strike RemcosRAT_807942ef	This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is 807942ef0aa75b3e4a16357df18004bc.

<b>Name</b>	<b>Description</b>
Strike RemcosRAT_8c080870	<p>This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is 8c0808705c8abff0a07a6ca91c6df24e.</p>
Strike RemcosRAT_8f70e913	<p>This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is 8f70e913513b30a144165829ba3261bb.</p>
Strike RemcosRAT_a86a836f	<p>This strike sends a polymorphic malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The binary has random bytes appended at the end of the file. The MD5 hash of this RemcosRAT sample is a86a836fc04ddabe4d35d3f240051915.</p>
Strike RemcosRAT_a9489436	<p>This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is a9489436209423d6472faa8b2151059d.</p>

<b>Name</b>	<b>Description</b>
Strike RemcosRAT_acc101b0	<p>This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is acc101b06dee1bb3c2e0a09fc08ad399.</p>
Strike RemcosRAT_bb4891f8	<p>This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is bb4891f869395e5eea518381e2f7ac42.</p>
Strike RemcosRAT_ca84ab08	<p>This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is ca84ab08e81d06ffaf20d8ed709ce136.</p>
Strike RemcosRAT_d2db8289	<p>This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is d2db828942b57a1d8b75297e3f493ef6.</p>
Strike RemcosRAT_d60fa5f2	<p>This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is d60fa5f203a8917e5bc3265af706b9c3.</p>

Name	Description
Strike RemcosRAT_d7ec95f3	This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is d7ec95f3bd2b9dd7b69aa50e8dbc990f.
Strike RemcosRAT_e2994fd1	This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is e2994fd1d2f56f8352ebf4d30b221d8f.
Strike RemcosRAT_f6118a96	This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is f6118a965e44ee55e708edf7adc1df.
Strike RemcosRAT_fe4e41fa	This strike sends a malware sample known as RemcosRAT. RemcosRAT is a malware that infiltrates systems through webhards in South Korea. It initially disguised as a legitimate remote administration tool, has transformed into a potent weapon for unauthorized remote control and data exfiltration. Threat actors lure users with seemingly harmless content, like adult games, containing a malicious VBS file. Upon execution, the VBS file connects to a remote service, initiating RemcosRAT download. Once installed, the malware compromises the user's system, granting remote access. It can tap into cameras and microphones, posing a serious privacy threat. The MD5 hash of this RemcosRAT sample is fe4e41fa88292d8be48fddfa6b0c0d7b.
Strike Remcos_0471eecc	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 0471eeccce6c5f38967035375fd45316.
Strike Remcos_0bdcea75	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 0bdcea756c30f97ad5181bd29bbb032a.

<b>Name</b>	<b>Description</b>
Strike Remcos_0da7c74e	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 0da7c74ea5d4521529b9c921529082b2.
Strike Remcos_10321543	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 10321543489147b3c45e9f04dc0911f4.
Strike Remcos_1188b7f5	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 1188b7f59772b41af3f9d5e9dd6070f2.
Strike Remcos_127c5d83	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Remcos sample is 127c5d833b841ae92fe87de4028595a3.
Strike Remcos_15751479	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 157514793080b82bf49b3c36acfa27ec.
Strike Remcos_179fc66a	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has been packed using upx packer, with the default options. The MD5 hash of this Remcos sample is 179fc66a0416442f19fe51271f5dfcfcd.
Strike Remcos_18eeb788	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has random bytes appended at the end of the file. The MD5 hash of this Remcos sample is 18eeb7888348eafcffa5024cec82b279.
Strike Remcos_1d8952fd	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 1d8952fd74a2f2fe021a977729c29377.
Strike Remcos_1f768b7d	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 1f768b7d743917bc837c5c354992181b.

<b>Name</b>	<b>Description</b>
Strike Remcos_21e43f1b	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Remcos sample is 21e43f1bec6e4eb7a86da442d462332c.
Strike Remcos_2eca497a	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 2eca497a11aec165cc35c112d6e3ce77.
Strike Remcos_305a77fb	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 305a77fbfb5624727c07ee5425e55e02.
Strike Remcos_31266fef	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 31266fefa52798b306939c3fc169c0ea.
Strike Remcos_31bbac78	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 31bbac78b447abc5a1138f5b0f3bb1ae.
Strike Remcos_33dff875	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 33dff875a64bdcca57f7c3d02bd7a0c0.
Strike Remcos_35629d91	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 35629d91d42d813e3bd6940439fb9ef2.
Strike Remcos_366831e3	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 366831e352b71d778262188d36f46810.
Strike Remcos_3798b258	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Remcos sample is 3798b25824964c133494cb323d6f8e44.
Strike Remcos_38db6cee	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 38db6ceeee8a5492b7dbdf4047148e86d.

<b>Name</b>	<b>Description</b>
Strike Remcos_41067caf	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 41067cafba34d8d865237bb22fa77c65.
Strike Remcos_439ef69b	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Remcos sample is 439ef69b62fefbe0324b799782f6ab7f.
Strike Remcos_44be3e0a	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 44be3e0a09970a7d85d158e24963765b.
Strike Remcos_451e8bc3	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Remcos sample is 451e8bc36e5cc304223cd137651a2ed8.
Strike Remcos_4635d673	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 4635d673c142cdf115c50a7dafdfcb7b.
Strike Remcos_4a236720	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 4a236720ee971788406f229e166e4a5a.
Strike Remcos_4afbe606	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 4afbe6063218a676ba3b745d71b6797c.
Strike Remcos_4ba7589c	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 4ba7589c1c9f38447e487d7dd670eac5.
Strike Remcos_4c82120c	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 4c82120c76135c0e7917ddc02f0985ff.
Strike Remcos_4d8b08ea	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 4d8b08eabce887328f433915339a5092.

<b>Name</b>	<b>Description</b>
Strike Remcos_524d430a	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has random bytes appended at the end of the file. The MD5 hash of this Remcos sample is 524d430a8844f33d9a054530d5a14cb2.
Strike Remcos_52910f26	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 52910f268831cf97d5d3f561052be6e5.
Strike Remcos_5b3b0765	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Remcos sample is 5b3b07657907de883d44735ac1c270df.
Strike Remcos_5f48006d	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 5f48006dfa96344985342dbc60d87c95.
Strike Remcos_5f4b0a0f	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 5f4b0a0fc9e6d760a09f5b87826e6212.
Strike Remcos_5ff832b3	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Remcos sample is 5ff832b37c2e809c3b7cf09ab9c94a2d.
Strike Remcos_6455a58b	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 6455a58b92b456e20c9bc66550c20e26.
Strike Remcos_66e37191	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 66e3719194f12a5f4636ce5010361d55.
Strike Remcos_66e4497c	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 66e4497cda52ee1af35ec3bb0c54070f.

<b>Name</b>	<b>Description</b>
Strike Remcos_6aa873ee	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 6aa873ee68b60704e3d00f5c885a90f7.
Strike Remcos_6abcaacb	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 6abcaacb64cc513284039899ac1f47af.
Strike Remcos_6b171762	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 6b171762ebb3aa6d0dfd8df3dc97f3bf.
Strike Remcos_6c09e425	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 6c09e425911932528d9fa31d02eaa04e.
Strike Remcos_71851026	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 7185102663f9ac5bccbf6744c51ae79.
Strike Remcos_71e06b1c	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 71e06b1c970a50e9c6ad29d3d54beb5b.
Strike Remcos_7228b27d	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 7228b27d20e6c526fa28b54795f6d7cf.
Strike Remcos_755ae12d	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 755ae12d9f12fc76f382ec1282faa029.
Strike Remcos_75923cf6	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Remcos sample is 75923cf648fa5660efe855589465266f9.
Strike Remcos_769fed4d	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 769fed4d63791d8a4b8ce332b916cd5e.

<b>Name</b>	<b>Description</b>
Strike Remcos_78d368e7	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 78d368e75f05884ee1bc41eaae669a5d.
Strike Remcos_7ea4e9cb	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 7ea4e9cb4550062b614f0b40c48445ed.
Strike Remcos_7ed789c2	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 7ed789c2fdb735bc813def6209270de1.
Strike Remcos_7f0579cf	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 7f0579cf11e45669bc3308e7c70d8dff.
Strike Remcos_7faf8334	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 7faf83341e5db899efe051b69a718045.
Strike Remcos_8311f9ad	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has random bytes appended at the end of the file. The MD5 hash of this Remcos sample is 8311f9ad5b8e1ec06c2f1a4aae3a11c9.
Strike Remcos_85374450	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 853744502b68e50e6cbaf81ffb3f5cc0.
Strike Remcos_85bb2be3	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 85bb2be314bb8b687e5c7763d69ff3a3.
Strike Remcos_884a4651	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 884a4651833f93ba58584cd89049c4c1.
Strike Remcos_89affee5	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 89affee5f44a964e2cc9fcabeb5a1a0f.

<b>Name</b>	<b>Description</b>
Strike Remcos_8b826147	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 8b82614718840850e60c517764308761.
Strike Remcos_8dc78c20	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 8dc78c2031bb121b86c4646e27aeb308.
Strike Remcos_9263fd64	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 9263fd6434fb0b0c0c2a7851b4e32e66.
Strike Remcos_99548f77	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 99548f77a249924a7355728f3ba1c328.
Strike Remcos_9dac209f	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is 9dac209f01d5275305d9a3fd41bab452.
Strike Remcos_a075d07d	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is a075d07dffdf125e20a57048deaa8abc.
Strike Remcos_a6725728	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is a6725728d876de2468707a0e2609edad.
Strike Remcos_a6a8faa7	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is a6a8faa704754eaac8d6642ad5880efd.
Strike Remcos_a902c80f	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Remcos sample is a902c80fcb532b5baf357a4b6a6583ec.
Strike Remcos_abdd03ce	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is abdd03cef2d854d4caa2b633d633bfe1.

<b>Name</b>	<b>Description</b>
Strike Remcos_b1fea42d	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is b1fea42d2bec29cc100f5cd47262c1cf.
Strike Remcos_b3091615	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is b30916158dd59d297781517b163162f7.
Strike Remcos_b37cbd5b	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is b37cbd5bde82458f0c0ad7ab45db03c2.
Strike Remcos_b8215d5a	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is b8215d5a8fbe30b59212bdde97e70c73.
Strike Remcos_b894f153	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is b894f153a0709c763352d3fd05c0bb19.
Strike Remcos_baf812e1	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is baf812e1e971741fb5e0f66611632683.
Strike Remcos_bde02894	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is bde0289473fa5ed70ff343254bbb5c76.
Strike Remcos_bf946994	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Remcos sample is bf946994b17dac838ce6914c92c348f3.
Strike Remcos_c1c492e4	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is c1c492e4f1f7b03c1dc72aae33df2ef.
Strike Remcos_c836f9a2	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is c836f9a28457c02bff3369ee5f1c4c8e.

<b>Name</b>	<b>Description</b>
Strike Remcos_cb7772f1	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Remcos sample is cb7772f18d7998fb440e4a7531a1da64.
Strike Remcos_cbca03f7	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is cbca03f7d4b73b42caf9d613050dc414.
Strike Remcos_d006c280	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has random bytes appended at the end of the file. The MD5 hash of this Remcos sample is d006c28009f6706e5f5c10237b353229.
Strike Remcos_d0c458a8	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is d0c458a86b5132616ef03797c1ccb65a.
Strike Remcos_d4ea4101	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is d4ea41012f338b1b6f61f93d566ec97d.
Strike Remcos_d51f3fb7	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has been packed using upx packer, with the default options. The MD5 hash of this Remcos sample is d51f3fb7d1a86142f95423241b76abf8.
Strike Remcos_d5bf288b	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is d5bf288bbdf4afba177785a1511f1856.
Strike Remcos_d83dc6e6	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is d83dc6e6c5760a053e59307f5a69f6d8.
Strike Remcos_de67536a	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Remcos sample is de67536a7c57c981c32c16529560eb6b.

<b>Name</b>	<b>Description</b>
Strike Remcos_e3eb514a	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is e3eb514abb6b01dac51031b00c9426b8.
Strike Remcos_e6423276	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is e6423276771b55ea6c6fe28880a9a31d.
Strike Remcos_e6c802e9	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is e6c802e9f43228c9a1046c6060334d95.
Strike Remcos_e8ded79a	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is e8ded79af9b2b51bce510aeced4bef18.
Strike Remcos_e9564e92	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has been packed using upx packer, with the default options. The MD5 hash of this Remcos sample is e9564e9206c1d3172dec7f0100e4ea5f.
Strike Remcos_ea590f4a	This strike sends a polymorphic malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Remcos sample is ea590f4aece0afd09719e690201e73c2.
Strike Remcos_ecee832e	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is eccee832e996ffefdbb4cf87cee4ed906.
Strike Remcos_ed06f450	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is ed06f450120f6c02cb4e0518223686b7.
Strike Remcos_eeb78134	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is eeb78134f1bedb33f26d26059d5de140.

<b>Name</b>	<b>Description</b>
Strike Remcos_f64bc692	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is f64bc6923c8051b1cb7e9126c4725bf1.
Strike Remcos_f678dcff	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is f678dcff5c1bd21ee75c90faaa852bbd.
Strike Remcos_fba106ad	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is fba106ad4a1e85d868858350f0aa8574.
Strike Remcos_fbcad086	This strike sends a malware sample known as Remcos. Remcos is a RAT that logs keystrokes, and performs other interactions with the host like capturing screenshots. It is typically delivered via documents with macros in phishing emails. The MD5 hash of this Remcos sample is fbcd086e0b20b839ce4f29362624146.
Strike RevengeRAT_057203a5	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has the debug flag removed in the PE file format. The MD5 hash of this RevengeRAT sample is 057203a509074d89e126e35f42312d4b.
Strike RevengeRAT_0f01bb00	This strike sends a malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The MD5 hash of this RevengeRAT sample is 0f01bb00e77961cc09654252c4e36d2d.
Strike RevengeRAT_258cc018	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has been packed using upx packer, with the default options. The MD5 hash of this RevengeRAT sample is 258cc01818963e63732b831e3f3dad48.
Strike RevengeRAT_2e733b70	This strike sends a malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The MD5 hash of this RevengeRAT sample is 2e733b705772af545754a2440ba389ce.
Strike RevengeRAT_3a55316d	This strike sends a malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The MD5 hash of this RevengeRAT sample is 3a55316dc3fd3a6a2c0cee0a5a6f1dbe.

<b>Name</b>	<b>Description</b>
Strike RevengeRAT_43284076	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this RevengeRAT sample is 432840760b2cf2fe3ef45abcfcef07bc.
Strike RevengeRAT_44d87bf5	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has random bytes appended at the end of the file. The MD5 hash of this RevengeRAT sample is 44d87bf5878aa4257c5c2c6af15bb8db.
Strike RevengeRAT_4ba21ad1	This strike sends a malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The MD5 hash of this RevengeRAT sample is 4ba21ad15a2c38126ba154f8078d2131.
Strike RevengeRAT_4e5e0003	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this RevengeRAT sample is 4e5e00034ec3a51d8d731ace8e04dd2e.
Strike RevengeRAT_510b5279	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has the timestamp field updated in the PE file header. The MD5 hash of this RevengeRAT sample is 510b52794a54b51b72198cc7a0eb89d6.
Strike RevengeRAT_5a665a69	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has the timestamp field updated in the PE file header. The MD5 hash of this RevengeRAT sample is 5a665a69e8f3180ac2c04ec271c87271.
Strike RevengeRAT_6068ec4e	This strike sends a malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The MD5 hash of this RevengeRAT sample is 6068ec4eb917651127c8dcc9d090b7e8.
Strike RevengeRAT_61384796	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has been packed using upx packer, with the default options. The MD5 hash of this RevengeRAT sample is 61384796b20744038ffee8c26dde1c4e.

<b>Name</b>	<b>Description</b>
Strike RevengeRAT_673ab09f	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has the checksum removed in the PE file format. The MD5 hash of this RevengeRAT sample is 673ab09f65cd381878a411d811b33c48.
Strike RevengeRAT_71c2d8f9	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this RevengeRAT sample is 71c2d8f9e948838355e13f403044c55c.
Strike RevengeRAT_73148dd7	This strike sends a malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The MD5 hash of this RevengeRAT sample is 73148dd7ec9cb121dff247d30280b347.
Strike RevengeRAT_7e7b0eb7	This strike sends a malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The MD5 hash of this RevengeRAT sample is 7e7b0eb7d5c3a3468dd17aace7547690.
Strike RevengeRAT_82dedaa1	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has the debug flag removed in the PE file format. The MD5 hash of this RevengeRAT sample is 82dedaa1e502a7802defbbd5ef55d016.
Strike RevengeRAT_88f5f3c1	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this RevengeRAT sample is 88f5f3c1ab16bdccb3dc0fecd215c989.
Strike RevengeRAT_89c01ccf	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has the checksum removed in the PE file format. The MD5 hash of this RevengeRAT sample is 89c01ccf1c7c0b0a67b815b90ce9d2ba.
Strike RevengeRAT_91b1f030	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has the checksum removed in the PE file format. The MD5 hash of this RevengeRAT sample is 91b1f0305ef23617077ecfee3c88d4cd.

<b>Name</b>	<b>Description</b>
Strike RevengeRAT_9b00e7bc	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this RevengeRAT sample is 9b00e7bccdc12ad11431680b04704cbf.
Strike RevengeRAT_9d75003a	This strike sends a malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The MD5 hash of this RevengeRAT sample is 9d75003a3bef8075be960c60fe1e879b.
Strike RevengeRAT_a313ea0f	This strike sends a malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The MD5 hash of this RevengeRAT sample is a313ea0fed0403239f5d88fce896d605.
Strike RevengeRAT_a6a78a35	This strike sends a malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The MD5 hash of this RevengeRAT sample is a6a78a35d3b3de48b8aec29aa9d82baf.
Strike RevengeRAT_bebe4275	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this RevengeRAT sample is bebe427531c6100a79c711fcaaaded48.
Strike RevengeRAT_c02d9cb8	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has random bytes appended at the end of the file. The MD5 hash of this RevengeRAT sample is c02d9cb84c68fc95e0e1ec197ed08084.
Strike RevengeRAT_cb833676	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has been packed using upx packer, with the default options. The MD5 hash of this RevengeRAT sample is cb833676d38a127902152901c483e5a1.
Strike RevengeRAT_d9f59ce8	This strike sends a malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The MD5 hash of this RevengeRAT sample is d9f59ce8bd678fff3e786b7fa4cf1b82.

<b>Name</b>	<b>Description</b>
Strike RevengeRAT_de9ffed8	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has the debug flag removed in the PE file format. The MD5 hash of this RevengeRAT sample is de9ffed898644efb8a97cbe13c5409c4.
Strike RevengeRAT_e0a1c381	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this RevengeRAT sample is e0a1c381ad9f1b6de631b70e16d606e9.
Strike RevengeRAT_e0bbff0c	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this RevengeRAT sample is e0bbff0cb922171a5066a9b5a22ddada.
Strike RevengeRAT_e4e4a363	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has random bytes appended at the end of the file. The MD5 hash of this RevengeRAT sample is e4e4a363ba46ee1d59689cbc1dbd7e13.
Strike RevengeRAT_e588b115	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has the timestamp field updated in the PE file header. The MD5 hash of this RevengeRAT sample is e588b11572ffbfe9eef1765bf9f1362b.
Strike RevengeRAT_e5e2ab4c	This strike sends a malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The MD5 hash of this RevengeRAT sample is e5e2ab4ccc365f5ddda84e609d62a71c.
Strike RevengeRAT_efd1e125	This strike sends a polymorphic malware sample known as RevengeRAT. This sample is a Remote Access Tool that allows for the attacker to perform a variety of malicious covert functions on the target system. Some of these capabilities include but are not limited to, spying on the user, and ex-filtrating data. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this RevengeRAT sample is efd1e1254bb1cf34b663a56dfbfd028.

<b>Name</b>	<b>Description</b>
Strike Rhysida_0c8e8887	This strike sends a malware sample known as Rhysida. Rhysida is ransomware that claims to be a cybersecurity team informing the victim about their system being compromised, and claiming to help them. The malware itself has been delivered via phishing and dropped as additional malware from frameworks like Cobalt Strike. The malware not only encrypts the system files, but the group appears to also exfiltrate data from the victims. The MD5 hash of this Rhysida sample is 0c8e88877383ccd23a755f429006b437.
Strike Rhysida_1e256229	This strike sends a malware sample known as Rhysida. Rhysida is ransomware that claims to be a cybersecurity team informing the victim about their system being compromised, and claiming to help them. The malware itself has been delivered via phishing and dropped as additional malware from frameworks like Cobalt Strike. The malware not only encrypts the system files, but the group appears to also exfiltrate data from the victims. The MD5 hash of this Rhysida sample is 1e256229b58061860be8dbf0dc4fe67e.
Strike Rhysida_41948cd7	This strike sends a malware sample known as Rhysida. Rhysida is ransomware that claims to be a cybersecurity team informing the victim about their system being compromised, and claiming to help them. The malware itself has been delivered via phishing and dropped as additional malware from frameworks like Cobalt Strike. The malware not only encrypts the system files, but the group appears to also exfiltrate data from the victims. The MD5 hash of this Rhysida sample is 41948cd77a6cf817b77be426968a6ad3.
Strike Rhysida_44c7d186	This strike sends a malware sample known as Rhysida. Rhysida is ransomware that claims to be a cybersecurity team informing the victim about their system being compromised, and claiming to help them. The malware itself has been delivered via phishing and dropped as additional malware from frameworks like Cobalt Strike. The malware not only encrypts the system files, but the group appears to also exfiltrate data from the victims. The MD5 hash of this Rhysida sample is 44c7d18633b5741db270a6bd378b6f3c.
Strike Rhysida_4ef0160b	This strike sends a malware sample known as Rhysida. Rhysida is ransomware that claims to be a cybersecurity team informing the victim about their system being compromised, and claiming to help them. The malware itself has been delivered via phishing and dropped as additional malware from frameworks like Cobalt Strike. The malware not only encrypts the system files, but the group appears to also exfiltrate data from the victims. The MD5 hash of this Rhysida sample is 4ef0160b3eb114a94aeedd0bb5716058.
Strike Rhysida_599aa41f	This strike sends a malware sample known as Rhysida. Rhysida is ransomware that claims to be a cybersecurity team informing the victim about their system being compromised, and claiming to help them. The malware itself has been delivered via phishing and dropped as additional malware from frameworks like Cobalt Strike. The malware not only encrypts the system files, but the group appears to also exfiltrate data from the victims. The MD5 hash of this Rhysida sample is 599aa41fade39e06daf4cdc87bb78bd7.
Strike Rhysida_59a9ca79	This strike sends a malware sample known as Rhysida. Rhysida is ransomware that claims to be a cybersecurity team informing the victim about their system being compromised, and claiming to help them. The malware itself has been delivered via phishing and dropped as additional malware from frameworks like Cobalt Strike. The malware not only encrypts the system files, but the group appears to also exfiltrate data from the victims. The MD5 hash of this Rhysida sample is 59a9ca795b59161f767b94fc2dece71a.

<b>Name</b>	<b>Description</b>
Strike Rhysida_c9a5e675	This strike sends a malware sample known as Rhysida. Rhysida is ransomware that claims to be a cybersecurity team informing the victim about their system being compromised, and claiming to help them. The malware itself has been delivered via phishing and dropped as additional malware from frameworks like Cobalt Strike. The malware not only encrypts the system files, but the group appears to also exfiltrate data from the victims. The MD5 hash of this Rhysida sample is c9a5e675dbb1f0ce61623f24757a1c72.
Strike Rhysida_fbbb2685	This strike sends a malware sample known as Rhysida. Rhysida is ransomware that claims to be a cybersecurity team informing the victim about their system being compromised, and claiming to help them. The malware itself has been delivered via phishing and dropped as additional malware from frameworks like Cobalt Strike. The malware not only encrypts the system files, but the group appears to also exfiltrate data from the victims. The MD5 hash of this Rhysida sample is fbbb2685cb612b25c50c59c1ffa6e654.
Strike RoamingMouse_016df9e0	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 016df9e04a1cb43d5d109dcc5144f4b.
Strike RoamingMouse_0d5f387e	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 0d5f387e8390673c598791398a0f075a.
Strike RoamingMouse_14369bdc	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 14369bdc5db99e074e7c46c534fd4ff4.

<b>Name</b>	<b>Description</b>
Strike RoamingMouse_1450f053	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 1450f0538fd02131b8c1965a7dfa562c.
Strike RoamingMouse_306504ab	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 306504ab7aa2eaee1a5a6bb29c698e70.
Strike RoamingMouse_316e987d	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 316e987dc5ea77113e288db3fb3e9f6.
Strike RoamingMouse_36bccf5b	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 36bccf5b8a86dd273edd936e2c56e942.
Strike RoamingMouse_3de5e596	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 3de5e5969683d69dfd970ec6b64f7421.

<b>Name</b>	<b>Description</b>
Strike RoamingMouse_41ac3590	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 41ac35900ca114695acb03d9639fd946.
Strike RoamingMouse_4ae5a008	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 4ae5a0088ae29edc09eb4c37c404622c.
Strike RoamingMouse_4ecc6467	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 4ecc6467a725d7bef6264ef5ca307a07.
Strike RoamingMouse_51face5b	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 51face5b20d783d384c479d1e975b0d1.
Strike RoamingMouse_63b84843	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 63b84843bf2832538b750313f66f97f4.

<b>Name</b>	<b>Description</b>
Strike RoamingMouse_63ea221b	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 63ea221bdb8e1d125e2eb199b053f56e.
Strike RoamingMouse_6bb0a90d	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 6bb0a90d607bd94bae417b45a3ea078.
Strike RoamingMouse_713627d0	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 713627d04dc027cbeeab77c3b128e5a9.
Strike RoamingMouse_7be8712c	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 7be8712c3f5646f2be68ed778a27e83b.
Strike RoamingMouse_7f90e779	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 7f90e7798f13bd496c9c4ffe9b33bbd5.

<b>Name</b>	<b>Description</b>
Strike RoamingMouse_96fa615e	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is 96fa615e523d689bff1449de9a4c5d28.
Strike RoamingMouse_d462fb86	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is d462fb86f928005214c7368d726d8472.
Strike RoamingMouse_d5ea3247	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is d5ea3247d0452965cad84fa1fc9f1e1a.
Strike RoamingMouse_e1c4fbe1	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is e1c4fbe183620334932ae8dffabfd7d.
Strike RoamingMouse_e6396a5f	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is e6396a5fe95fccabe5bf4ea30bc14d92.

<b>Name</b>	<b>Description</b>
Strike RoamingMouse_e795ac19	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is e795ac19d2ea70e1e3a8e048299dccb6.
Strike RoamingMouse_efd6eb55	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is efd6eb554cf39d0b323d80e64986f0dd.
Strike RoamingMouse_f81c604b	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is f81c604b015d1e9abc629d46cf476786.
Strike RoamingMouse_fc9fb323	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is fc9fb323b449ee20c24e994961cd7a67.
Strike RoamingMouse_fe6126a0	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is fe6126a0e6b25e95827c0a820d9f3d25.

<b>Name</b>	<b>Description</b>
Strike RoamingMouse_fef77348	This strike sends a malware sample known as RoamingMouse. RoamingMouse is a macro enabled dropper that drops various malicious components. These variants were seen in Excel files and are triggered via mouse click events. In the case of the Earth Kasha 2025 campaign the malicious components roamingmouse drops are legitimate signed applications and dlls from JustSystems Inc, as well as a malicious ANELLDR loader and encrypted ANEL payload. Once the user clicks the macro and execution of roamingmouse begins, the legitimate dropped .exe is launched from explorer.exe and then side loads the malicious dll in the same directory. The MD5 hash of this RoamingMouse sample is fef77348affd4ee3e201366381dede30.
Strike Ruskill_06186a2f	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 06186a2f936fee608094cf074e49072b.
Strike Ruskill_08417575	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 0841757582ec90c1aa0b2e5dcfa18a10.
Strike Ruskill_1d1bccd2	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 1d1bccd23b7cf435334f34766ffb6858.
Strike Ruskill_1df989f0	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 1df989f01c373dcdaa768e1d616c4ee1.
Strike Ruskill_2671866d	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 2671866d29ef60cef7d2543a72d4fa05.
Strike Ruskill_2824fdeb	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 2824fdebf4c8188c6128cd06a403da6a.
Strike Ruskill_2d3f70b0	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 2d3f70b08c4d9a3c4ac2d2065dbb1130.
Strike Ruskill_3ed76c13	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 3ed76c13d2dee62a1b707530a744354c.

<b>Name</b>	<b>Description</b>
Strike Ruskill_4674372d	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 4674372dfcdbeef581d50685083ec0f4.
Strike Ruskill_4cc1fdf0	This strike sends a polymorphic malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The binary has the checksum removed in the PE file format. The MD5 hash of this Ruskill sample is 4cc1fdf07ade397fe202ff10dcd9d1d3.
Strike Ruskill_52479cdd	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 52479cdd528eaeb80b34602492607c8f.
Strike Ruskill_62b6204d	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 62b6204d3fa543db17027c918b300e83.
Strike Ruskill_653db921	This strike sends a polymorphic malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Ruskill sample is 653db92104917aa366ce680b9ac563dc.
Strike Ruskill_688624dd	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 688624ddab6d450d24a7a6c317de6cc3.
Strike Ruskill_8935551d	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 8935551d375c42018bcef423006fcfd5.
Strike Ruskill_8b761275	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 8b761275be3448835ca45f2c089721b9.
Strike Ruskill_8c9b501a	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 8c9b501a908efe3ba7d828d7b51a6c9c.
Strike Ruskill_949c9314	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 949c93148b31f353b564ead90bc2644d.

<b>Name</b>	<b>Description</b>
Strike Ruskill_9c91abff	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is 9c91abff2ec28b11d6a188a865d37ff9.
Strike Ruskill_b3a7b671	This strike sends a polymorphic malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The binary file has one more imports added in the import table. The MD5 hash of this Ruskill sample is b3a7b6717595d216675b92c351502193.
Strike Ruskill_b804afd1	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is b804afd1fc915ef1e78e2343d2024800.
Strike Ruskill_b9b6030c	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is b9b6030c56aff5136cd86f88cef141eb.
Strike Ruskill_be5e43f2	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is be5e43f2786d628b7aa8689c2108247d.
Strike Ruskill_c217a53d	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is c217a53dcba7dd40209b16909d2dabe9.
Strike Ruskill_c5c85a5d	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is c5c85a5dec6e85e0987dc77534cd2245.
Strike Ruskill_cbeaa60d	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is cbeaa60d3ca9e95aa97ced332046597f.
Strike Ruskill_d873e514	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is d873e514a8b483b31a49d6063b4d3522.
Strike Ruskill_d8c2cb4d	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is d8c2cb4d206da999ba787f961e46db89.

<b>Name</b>	<b>Description</b>
Strike Ruskill_de840601	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is de840601a818c3b2bfce3828ad10ab78.
Strike Ruskill_f12998e1	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is f12998e1874bfbad5103305a910e6a45.
Strike Ruskill_f8169d67	This strike sends a malware sample known as Ruskill. Ruskill is a botnet that spreads via removable media and through messaging applications. It steals credentials and distributes denial of service attacks. The MD5 hash of this Ruskill sample is f8169d674fa96973c0b37a0e4524d497.
Strike Ryuk_04639dd8	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 04639dd868345e24c767c8a153593436.
Strike Ryuk_071d4716	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Ryuk sample is 071d4716a409b086872bdbe837a31d7b.
Strike Ryuk_0bb638bd	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 0bb638bd51b766e8b9d7ad49c56153fc.
Strike Ryuk_0fc372ad	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 0fc372ad8300d566a4cbe89b9366e57e.
Strike Ryuk_104f6f8b	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 104f6f8b721d8e6e5e724158def0eb18.
Strike Ryuk_13b49e7e	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 13b49e7ec53399818737a28259061ca6.

<b>Name</b>	<b>Description</b>
Strike Ryuk_13c8f412	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 13c8f41211cc5295cf72b636cc8310a8.
Strike Ryuk_1505c34d	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 1505c34d9db1d458f4552ba34020fc7d.
Strike Ryuk_154b73d0	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 154b73d0a7aa19df12364a78b235f29f.
Strike Ryuk_161adc64	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 161adc6440a1deb1adfb6bdb1debe0fa.
Strike Ryuk_16689765	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 1668976511b5c77bfba8a77a392fe1a1.
Strike Ryuk_19d19635	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 19d19635ad37caef4bf498bd082c6617.
Strike Ryuk_1c61d7e8	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Ryuk sample is 1c61d7e8ec2eb2d1dd9f7fce77a65740.
Strike Ryuk_1d3b545a	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Ryuk sample is 1d3b545a4eeaebf971a071e3573a88f9.

<b>Name</b>	<b>Description</b>
Strike Ryuk_230fe4f6	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 230fe4f6a5ca6f6e0e7995a4c4e7c571.
Strike Ryuk_2c754773	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has the debug flag removed in the PE file format. The MD5 hash of this Ryuk sample is 2c754773e8670230e2c7939e96d6b3eb.
Strike Ryuk_2f57a84c	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Ryuk sample is 2f57a84ccae324e47e59a056469dc2ae.
Strike Ryuk_3266352b	This strike sends a malware sample known as Ryuk. Ryuk is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 3266352bea7513ac3ead6e7d68661ad3.
Strike Ryuk_3303bc82	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Ryuk sample is 3303bc8283ac6735d4dddae5ffc6ceab.
Strike Ryuk_34caab0d	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 34caab0dfb3c757ea2b109a594283b9f.
Strike Ryuk_35194c73	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 35194c73ff38dd6c3bed7c0efcff6826.
Strike Ryuk_3925ae7d	This strike sends a malware sample known as Ryuk. Ryuk is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 3925ae7df3328773be923f74d70555e3.

<b>Name</b>	<b>Description</b>
Strike Ryuk_3aacbe44	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Ryuk sample is 3aacbe448962a3892663a0001b4af7cb.
Strike Ryuk_40492c17	This strike sends a malware sample known as Ryuk. Ryuk is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 40492c178079e65dfd5449bf899413b6.
Strike Ryuk_4a2a67ec	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 4a2a67ecc78856db836acda48a1aa71.
Strike Ryuk_4e8f164c	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 4e8f164cfb304e5522c9cd940c7cbb7b.
Strike Ryuk_4ed8b68b	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has random bytes appended at the end of the file. The MD5 hash of this Ryuk sample is 4ed8b68b3bbea1d2c54ea5f2b0299842.
Strike Ryuk_5824da6d	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Ryuk sample is 5824da6dcacaf9bf531d9c0688b5da7e.
Strike Ryuk_5f7dd374	This strike sends a malware sample known as Ryuk. Ryuk is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 5f7dd3740a3a4ea74e2ee234f6de26aa.
Strike Ryuk_622bc38d	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 622bc38dee08e70e91e2be32a58b6d1f.

<b>Name</b>	<b>Description</b>
Strike Ryuk_67b3f1da	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 67b3f1da9c742db2648beced5c5bbbe5.
Strike Ryuk_6a5bf25f	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 6a5bf25ff4f72ebca91280ffda057260.
Strike Ryuk_75f27ff2	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 75f27ff22a3d049a00b0a6488c3c2607.
Strike Ryuk_792b7e90	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 792b7e90bda1e63ea362c8db420d3f6f.
Strike Ryuk_7fdbcb96e	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has random bytes appended at the end of the file. The MD5 hash of this Ryuk sample is 7fdbcb96ea01f7c0e4410014ce7b9127e.
Strike Ryuk_82e24ddd	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Ryuk sample is 82e24dddb83ec0349581f101b86c82dd.
Strike Ryuk_8b4bb879	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is 8b4bb8791c66ad542a2116b1c8371168.
Strike Ryuk_a57e1e6f	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is a57e1e6fe1c98d2e75799a46e9eb5797.

<b>Name</b>	<b>Description</b>
Strike Ryuk_a650d567	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is a650d5676dc2c91a3af2216044ddaf8c.
Strike Ryuk_ae9eebd8	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is ae9eebd89da10a1724576ae492623e99.
Strike Ryuk_b00e7c8a	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is b00e7c8af8bc56372715b049d58e3b2d.
Strike Ryuk_b1c7f17b	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is b1c7f17b1eccde5397c5e1a464c79c42.
Strike Ryuk_b9ae09f8	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is b9ae09f838161b75747dfc02e414843c.
Strike Ryuk_ba6fb9d4	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is ba6fb9d42ae9e6afac4f40a273e85027.
Strike Ryuk_bf9236a4	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Ryuk sample is bf9236a49a1ac24ad8411500b2bcf62d.
Strike Ryuk_c2302c23	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is c2302c2340f628030c6b4c96d2de8656.

<b>Name</b>	<b>Description</b>
Strike Ryuk_d0ded7d0	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is d0ded7d0e15610bb35bf9a2d635835a3.
Strike Ryuk_d7697d0d	This strike sends a malware sample known as Ryuk. Ryuk is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is d7697d0d692bd883e53036b906108d56.
Strike Ryuk_db2766c6	This strike sends a malware sample known as Ryuk. Ryuk is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is db2766c6f43c25951cdd38304d328dc1.
Strike Ryuk_e28c32a0	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is e28c32a0aa83313237cc8ab58d4b1182.
Strike Ryuk_eb03af1d	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Ryuk sample is eb03af1daa9f68a1244a7e061b9ecccc.
Strike Ryuk_ecd9d8ef	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is ecd9d8ef99eb9813fa4eced549ea4d88.
Strike Ryuk_f12cd6eb	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is f12cd6ebcfb81649ee67456508ad541a.
Strike Ryuk_f166adfe	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is f166adfe07f5f743cf5556d16cad4a9.

<b>Name</b>	<b>Description</b>
Strike Ryuk_f7c4bda3	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Ryuk sample is f7c4bda38702df9cc2231fa2197d5db3.
Strike Ryuk_f8d72179	This strike sends a polymorphic malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The binary has the debug flag removed in the PE file format. The MD5 hash of this Ryuk sample is f8d721791b6d143e00281c686cfbe3ac.
Strike Ryuk_fca20e17	This strike sends a malware sample known as Ryuk. Ryuk is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is fca20e17ce8c0c3f3c78d82c953472ed.
Strike Ryuk_fcdb3b05	This strike sends a malware sample known as Ryuk. This sample is a highly targeted ransomware attack that has infected numerous organizations world wide. The malware performs extensive network mapping, and hacking. Because it is targeted credential collection is required and takes place in advance. The MD5 hash of this Ryuk sample is fcdb3b05c314b59d61fcebc413dc142f.
Strike SDK_13ac2635	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 13ac2635f70981a33bc422b7b8a8b5fd.
Strike SDK_1afd6a2e	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 1afd6a2e005334df2b24175ec80d0742.
Strike SDK_287ddfa3	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 287ddfa34525de0556c521cf21115b9a.

<b>Name</b>	<b>Description</b>
Strike SDK_3c0eaeb3	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 3c0eaeb351d17d8ac1d42bdcf41178ad.
Strike SDK_6dab8bad	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 6dab8bad4349055397aa35f1a48e9c90.
Strike SDK_76d40886	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 76d40886dce0d57b99f7008afd5e19bf.
Strike SDK_78ebd502	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 78ebd502ed1221202398623fb8ee2dd9.
Strike SDK_8823adc0	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 8823adc0960b86986aa346c119bd41f7.

<b>Name</b>	<b>Description</b>
Strike SDK_91827d2f	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 91827d2f3ab34de6b5857dab88c9a363.
Strike SDK_9589482a	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 9589482ad6c81182968a9fcba0f7ceed.
Strike SDK_963e8b9f	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 963e8b9f4400e7ad7f73cdd14b5f1b87.
Strike SDK_9967784e	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is 9967784e01447928148ac24d7e4c8f3d.
Strike SDK_a4027650	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is a40276505836397427fc37e979a1f353.

<b>Name</b>	<b>Description</b>
Strike SDK_b253302c	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is b253302c5936ef4eb8c3fbe74026ded6.
Strike SDK_b6442835	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is b644283582d909cde0e9bf4baf42fd16.
Strike SDK_c32c66aa	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is c32c66aae96d1a48ecf0e37f2be29ef5.
Strike SDK_e1a20e6d	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is e1a20e6d49c837bac9d2b56aae71db40.
Strike SDK_e9754692	This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is e9754692659f4d39c4e8d5fe6cb51973.

<b>Name</b>	<b>Description</b>
Strike SDK_f2af8db5	<p>This strike sends a malware sample known as SDK. The malware described is a Software Development Kit (SDK) that is used to sell bandwidth. It does this by embedding itself in popular apps and then running in the background to sell the user's bandwidth without their knowledge. Once installed, it uses the device's Internet connection to run various tasks, including DDoS attacks, serving pirated content, or even Bitcoin mining. Its key capabilities include running in the background without the user's knowledge, selling bandwidth, and performing various tasks for the attacker. The MD5 hash of this SDK sample is f2af8db568f135cd9a788b7caff4d517.</p>
Strike SUBTLE-PAWS_03eacabd	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version. The MD5 hash of this SUBTLE-PAWS sample is 03eacabd7841a9c044edf7efe09e3273.</p>
Strike SUBTLE-PAWS_0df2774f	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version. The MD5 hash of this SUBTLE-PAWS sample is 0df2774f47a003077d1e1fb4d000514b.</p>
Strike SUBTLE-PAWS_11e456c1	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version. The MD5 hash of this SUBTLE-PAWS sample is 11e456c1a6a193a384bf8ee0c83398f4.</p>
Strike SUBTLE-PAWS_1950b7cf	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version. The MD5 hash of this SUBTLE-PAWS sample is 1950b7cfc347e03505327579a9e98b55.</p>

<b>Name</b>	<b>Description</b>
Strike SUBTLE-PAWS_21d566ce	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is 21d566ce1a962a0d912b84d241bee81d.</p>
Strike SUBTLE-PAWS_2dd0c184	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is 2dd0c1841e9cd23a497361d7dfdf3c26.</p>
Strike SUBTLE-PAWS_311a566e	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is 311a566ecd56c20b7b303c743e5c69df.</p>
Strike SUBTLE-PAWS_3a43dedb	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is 3a43dedb892365519136d6f0e46af506.</p>
Strike SUBTLE-PAWS_535beba0	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is 535beba088fd402ae3950eae4d6e7c00.</p>

<b>Name</b>	<b>Description</b>
Strike SUBTLE-PAWS_5a5ca3c8	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is 5a5ca3c8f0a1ef89f2b5f620434acb94.</p>
Strike SUBTLE-PAWS_5d00c292	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is 5d00c2922bcb8e713aed772f9e5f5c87.</p>
Strike SUBTLE-PAWS_7a468656	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is 7a468656e4ef81e6517eaae9126d4d86.</p>
Strike SUBTLE-PAWS_90cbc7c3	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is 90cbc7c3e0c101aeae2aeb8f39b7ea57.</p>
Strike SUBTLE-PAWS_95fb274b	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is 95fb274b8e9b18d75b8699ef02665969.</p>

<b>Name</b>	<b>Description</b>
Strike SUBTLE-PAWS_af5081a1	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is af5081a1c0f4bdbb13ac256657feff23.</p>
Strike SUBTLE-PAWS_c3e19fbf	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is c3e19fb6fc6299dd1e0cba17b1f06c6.</p>
Strike SUBTLE-PAWS_d18e71f9	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is d18e71f95e817668a4d284b329ceccf8.</p>
Strike SUBTLE-PAWS_d19ef43d	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is d19ef43d2bffa01bd0cc590d18286a6.</p>
Strike SUBTLE-PAWS_d86eedd8	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is d86eedd8a5c4d87879a8d2c9ffd44287.</p>

<b>Name</b>	<b>Description</b>
Strike SUBTLE-PAWS_db4eb992	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is db4eb9920f1a7f04ec226cc69d99da1b.</p>
Strike SUBTLE-PAWS_ebca940b	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is ebca940b5d676e42a86491188a62cd0f.</p>
Strike SUBTLE-PAWS_ee4a2217	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is ee4a2217bd56685602194e7127182c89.</p>
Strike SUBTLE-PAWS_eeae2db7	<p>This strike sends a malware sample known as SUBTLE-PAWS. SUBTLE-PAWS is a PowerShell-based backdoor that targets Ukraine. It is distributed through compressed files and possibly phishing emails. It leverages PowerShell for most of its code execution and achieves dynamic execution and persistence by storing and retrieving executable code from the Windows Registry. The malware establishes communication with a remote server for Command &amp; Control and spreads through removable media by creating malicious shortcuts. It employs obfuscation techniques and environment sensitivity to operate stealthily and adjust its behavior based on the detected OS version The MD5 hash of this SUBTLE-PAWS sample is eeaе2db7cf9cf9deb15c70fad26d76d0.</p>
Strike SambaSpy_0f3b46d4	<p>This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is 0f3b46d496bbf47e8a2485f794132b48.</p>

<b>Name</b>	<b>Description</b>
Strike SambaSpy_31006178	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is 31006178337f68913ce4cea5258e7905.
Strike SambaSpy_37381cdf	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is 37381cdffacf56b244f1d77dafc9eb37.
Strike SambaSpy_374b0011	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is 374b001152bff252812a8b837dad505c.
Strike SambaSpy_42b632be	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is 42b632be79d99a73bf0519f30936c255.
Strike SambaSpy_6e5cc1fa	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is 6e5cc1fa3d8fe306e025fdf94de988cc.
Strike SambaSpy_74d64e7f	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is 74d64e7f638852464089f31d960a0c35.
Strike SambaSpy_832b0d8d	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is 832b0d8dbae79133a0d791ecb19e87b5.

<b>Name</b>	<b>Description</b>
Strike SambaSpy_a86ba64b	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is a86ba64bef883f3339e567a8c40e5c2b.
Strike SambaSpy_b46f0c93	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is b46f0c93a0090877745615422342fac5.
Strike SambaSpy_b7b71a0b	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is b7b71a0b5256a3ff1358a66651e2a14a.
Strike SambaSpy_bf659ff1	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is bf659ff1cb2e10ef31546d9ed5dd9ab7.
Strike SambaSpy_c3771475	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is c37714756c4cdaa6e82fa2dcfc8af19.
Strike SambaSpy_d153006e	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is d153006e00884edf7d48b9fe05d83cb4.
Strike SambaSpy_d96964a4	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is d96964a42f8cbb839679effe5ffce430.

<b>Name</b>	<b>Description</b>
Strike SambaSpy_e4811f31	This strike sends a malware sample known as SambaSpy. SambaSpy RAT malware written in Java. This malware is highly obfuscated and exhibits a host of functionality including system and process management, keystroke logging, and clipboard content grabbing, browser credential exfiltration, and remote shell control. Besides being heavily obfuscated, much of its C2 communication is encrypted. The MD5 hash of this SambaSpy sample is e4811f317e4df202229847834512a453.
Strike Scar_01abda83	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 01abda83c026ff0fe5dedd293b9c12cb.
Strike Scar_0274c84c	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 0274c84cd3e88e0f60f8843f56b3a632.
Strike Scar_09b3dde0	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 09b3dde0483c4d3d61b29c4c9622fea6.
Strike Scar_0c6c38f7	This strike sends a polymorphic malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Scar sample is 0c6c38f795d373fc8f5fc07f908903c4.
Strike Scar_0f32fa41	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 0f32fa41e160bdb3ad0ce83daad79f75.
Strike Scar_1951faf5	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 1951faf55309f61702bcda986e5229bf.
Strike Scar_1ecbcd7c	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 1ecbcd7cb132b302d1987d6354639341.
Strike Scar_2008fa22	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 2008fa2210a7123f228d83616b5b206b.
Strike Scar_2033f6b7	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 2033f6b72b573bae14191c702d12bfab.
Strike Scar_20a3ed89	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 20a3ed89cdf16707930a21217f912b97.

<b>Name</b>	<b>Description</b>
Strike Scar_220ef7f4	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 220ef7f41f700600d04c3a8b64964900.
Strike Scar_27161106	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 271611065a218801f7869636ec844402.
Strike Scar_30a527e1	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 30a527e1edc2815eafc93d038c755f3d.
Strike Scar_3171bbe3	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 3171bbe396ea5bec0d85042f7e891677.
Strike Scar_33454c7f	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 33454c7f55343c4200bbf4f7b7fc767e.
Strike Scar_35ab4641	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 35ab4641aa1904672a8b211ffcc45d4e.
Strike Scar_36a91fe4	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 36a91fe472d4ddff1c296a3e798deed.
Strike Scar_3786118b	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 3786118bba547421d900ad3c1136fabc.
Strike Scar_4139d679	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 4139d6792f8a47e5d9e0fe1b434cadb5.
Strike Scar_4d3e4ff9	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 4d3e4ff9f638ab8e9b6a23c372c107b6.
Strike Scar_50e9db8d	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 50e9db8d9efe0597e7b8d9cbaa6d79c7.
Strike Scar_50ef4e47	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 50ef4e475ee9ccf98e596a606d9d32e4.

<b>Name</b>	<b>Description</b>
Strike Scar_55932750	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 5593275031b345882d5e64aa7c9bb728.
Strike Scar_628f4334	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 628f4334ccffc5726199ac0cdf0d31d1.
Strike Scar_6664c718	This strike sends a polymorphic malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Scar sample is 6664c718d5bb1dc98f97a91013a9f017.
Strike Scar_67bbf0d5	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 67bbf0d5bb33948dcfde61bf415fdb8c.
Strike Scar_6b1d7e40	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 6b1d7e4042b9a77daa058ae57dd4702a.
Strike Scar_7e089601	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 7e089601c83340ebdbaaef2a9d4ebb45.
Strike Scar_8628f5f1	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 8628f5f1d6593915cf23b60c46377cc1.
Strike Scar_874499a9	This strike sends a polymorphic malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The binary has been packed using upx packer, with the default options. The MD5 hash of this Scar sample is 874499a974acb34d4827b6e1a91143d6.
Strike Scar_8c15f415	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 8c15f415f158443db22461bb7b4dc62e.
Strike Scar_91eb29c6	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 91eb29c6e9c065a0259b936101739b90.
Strike Scar_9adb6b64	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is 9adb6b64a3edeba039c4f45bee5bef.

<b>Name</b>	<b>Description</b>
Strike Scar_a3d952e7	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is a3d952e7057f8a0d89f6d846f46befa9.
Strike Scar_a9b07c69	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is a9b07c698d3a6ef0e1b6fee12cd2abfc.
Strike Scar_b1d50917	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is b1d50917fe432a627a56ad8045fa845c.
Strike Scar_c5cc2b2b	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is c5cc2b2bd4979d83a23297389e7a66b8.
Strike Scar_c96441e8	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is c96441e8d833155cc125c819d4ef680f.
Strike Scar_d1133bb1	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is d1133bb179cf07980c1b118ae16c6b2f.
Strike Scar_d2522dc0	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is d2522dc08fd312cbd1104d7fe2086656.
Strike Scar_d71c3fe6	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is d71c3fe641a6e1379ec2648d524de8f0.
Strike Scar_db3b2e97	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is db3b2e97fdc5cb7c4c830d937475a0e5.
Strike Scar_ddd4f409	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is ddd4f4098ac6f562a1933aaeb3f764e6.
Strike Scar_e4f3dfb4	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is e4f3dfb4b4fd91b082f8d58a6d25befc.
Strike Scar_e6511a4a	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is e6511a4aee70c7d7a9c5619167d925ee.

<b>Name</b>	<b>Description</b>
Strike Scar_e9bd79bb	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is e9bd79bb61fc7ac4f4ff2dea03751bc1.
Strike Scar_ebaed22b	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is ebaed22b81e90153fc2ad70098604ae2.
Strike Scar_f740c3dd	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is f740c3dd1532b687d451dcc4f63ecfd3.
Strike Scar_f8396a17	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is f8396a17869a29e9f125e8459327d954.
Strike Scar_f90256f5	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is f90256f556b2743291103bbaa4f66302.
Strike Scar_ff9bd65f	This strike sends a malware sample known as Scar. Scar is a worm and will download files while also trying to spread to other machines by copying itself to removable media. The MD5 hash of this Scar sample is ff9bd65f29492a559e2f630afbe9accd.
Strike Sekhmet_1343bd0e	This strike sends a malware sample known as Sekhmet. The Sekhmet ransomware was used in an attack against gas handling company SilPac in June 2020. This ransomware has been commonly spread via spam email. Once it encrypts the files on the targeted system it leaves behind a RECOVER-FILES.txt file that includes a ransom note with instructions on how to pay via TOR. The MD5 hash of this Sekhmet sample is 1343bd0e55191ff224f2a5d4b30cdf3b.
Strike Sekhmet_b7ad5f7e	This strike sends a malware sample known as Sekhmet. The Sekhmet ransomware was used in an attack against gas handling company SilPac in June 2020. This ransomware has been commonly spread via spam email. Once it encrypts the files on the targeted system it leaves behind a RECOVER-FILES.txt file that includes a ransom note with instructions on how to pay via TOR. The MD5 hash of this Sekhmet sample is b7ad5f7ec71dc812b4771950671b192a.
Strike Shikitega_04ad59ff	This strike sends a malware sample known as Shikitega. Shikitega is malware that targets devices that running the Linux OS. It is delivered in a multistage infection chain where each module responds to a part of the payload and then proceeds to download and execute the next module. When run a cryptominer is executed and the attacker can is potentially granted full access to the machine. The MD5 hash of this Shikitega sample is 04ad59ff2b2b8461a6d990af16bc5ca7.

<b>Name</b>	<b>Description</b>
Strike Shikitega_0f1f2d4a	This strike sends a malware sample known as Shikitega. Shikitega is malware that targets devices that running the Linux OS. It is delivered in a multistage infection chain where each module responds to a part of the payload and then proceeds to download and execute the next module. When run a cryptominer is executed and the attacker can is potentially granted full access to the machine. The MD5 hash of this Shikitega sample is 0f1f2d4a6fc26df7cf5d5a8c65ac8578.
Strike Shikitega_2f56a330	This strike sends a malware sample known as Shikitega. Shikitega is malware that targets devices that running the Linux OS. It is delivered in a multistage infection chain where each module responds to a part of the payload and then proceeds to download and execute the next module. When run a cryptominer is executed and the attacker can is potentially granted full access to the machine. The MD5 hash of this Shikitega sample is 2f56a330fb253a1520e00668c6f94e47.
Strike Shikitega_557bdc56	This strike sends a malware sample known as Shikitega. Shikitega is malware that targets devices that running the Linux OS. It is delivered in a multistage infection chain where each module responds to a part of the payload and then proceeds to download and execute the next module. When run a cryptominer is executed and the attacker can is potentially granted full access to the machine. The MD5 hash of this Shikitega sample is 557bdc5602b301d5584a34b27328b019.
Strike Shikitega_6b13e69c	This strike sends a malware sample known as Shikitega. Shikitega is malware that targets devices that running the Linux OS. It is delivered in a multistage infection chain where each module responds to a part of the payload and then proceeds to download and execute the next module. When run a cryptominer is executed and the attacker can is potentially granted full access to the machine. The MD5 hash of this Shikitega sample is 6b13e69cc37757b1f2dbc2a1c8f806f1.
Strike Shikitega_6e684589	This strike sends a malware sample known as Shikitega. Shikitega is malware that targets devices that running the Linux OS. It is delivered in a multistage infection chain where each module responds to a part of the payload and then proceeds to download and execute the next module. When run a cryptominer is executed and the attacker can is potentially granted full access to the machine. The MD5 hash of this Shikitega sample is 6e6845896222ee7d48e76ea2bf11b97d.
Strike Shikitega_7a34ca9c	This strike sends a malware sample known as Shikitega. Shikitega is malware that targets devices that running the Linux OS. It is delivered in a multistage infection chain where each module responds to a part of the payload and then proceeds to download and execute the next module. When run a cryptominer is executed and the attacker can is potentially granted full access to the machine. The MD5 hash of this Shikitega sample is 7a34ca9c59cde0af620ffa30783348a9.
Strike Shikitega_7b229d73	This strike sends a malware sample known as Shikitega. Shikitega is malware that targets devices that running the Linux OS. It is delivered in a multistage infection chain where each module responds to a part of the payload and then proceeds to download and execute the next module. When run a cryptominer is executed and the attacker can is potentially granted full access to the machine. The MD5 hash of this Shikitega sample is 7b229d73b7c5c55fda0e1f57ceaaf118.

<b>Name</b>	<b>Description</b>
Strike Shikitega_932df67e	This strike sends a malware sample known as Shikitega. Shikitega is malware that targets devices that running the Linux OS. It is delivered in a multistage infection chain where each module responds to a part of the payload and then proceeds to download and execute the next module. When run a cryptominer is executed and the attacker can is potentially granted full access to the machine. The MD5 hash of this Shikitega sample is 932df67ea6b8900a30249e311195a58f.
Strike Shikitega_b035f858	This strike sends a malware sample known as Shikitega. Shikitega is malware that targets devices that running the Linux OS. It is delivered in a multistage infection chain where each module responds to a part of the payload and then proceeds to download and execute the next module. When run a cryptominer is executed and the attacker can is potentially granted full access to the machine. The MD5 hash of this Shikitega sample is b035f85870bb17380b25189bd97b8e65.
Strike Shikitega_d1cd3293	This strike sends a malware sample known as Shikitega. Shikitega is malware that targets devices that running the Linux OS. It is delivered in a multistage infection chain where each module responds to a part of the payload and then proceeds to download and execute the next module. When run a cryptominer is executed and the attacker can is potentially granted full access to the machine. The MD5 hash of this Shikitega sample is d1cd3293ac4b312e0b3218e80376bd88.
Strike Shikitega_da193f6b	This strike sends a malware sample known as Shikitega. Shikitega is malware that targets devices that running the Linux OS. It is delivered in a multistage infection chain where each module responds to a part of the payload and then proceeds to download and execute the next module. When run a cryptominer is executed and the attacker can is potentially granted full access to the machine. The MD5 hash of this Shikitega sample is da193f6bf387f9884d88ace9c04278a0.
Strike Shikitega_fd3bc823	This strike sends a malware sample known as Shikitega. Shikitega is malware that targets devices that running the Linux OS. It is delivered in a multistage infection chain where each module responds to a part of the payload and then proceeds to download and execute the next module. When run a cryptominer is executed and the attacker can is potentially granted full access to the machine. The MD5 hash of this Shikitega sample is fd3bc823d9e6b1aa0622c36ebd5e69f2.
Strike Shiz_05656b0d	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 05656b0dd1f2c011d7b9e4f4de4f77a2.
Strike Shiz_07dbe784	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 07dbe7842a4dabd8c39f0af2bf1881d5.
Strike Shiz_09024d6e	This strike sends a polymorphic malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The binary has the checksum removed in the PE file format. The MD5 hash of this Shiz sample is 09024d6e756bc7200ba179a6aeb9f41d.

<b>Name</b>	<b>Description</b>
Strike Shiz_228ee144	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 228ee1443e6f972d2cb502a4a030aac5.
Strike Shiz_22e33d40	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 22e33d40c6a620d29ceeb324ef5b5f40.
Strike Shiz_277b47f8	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 277b47f81244411d20903be4d78dd5d9.
Strike Shiz_28329ecd	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 28329ecd0afc07c18ab89730c81e7790.
Strike Shiz_2ede41ce	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 2ede41ce1e9f83d50cc15b2e56f74ddc.
Strike Shiz_36cda7c7	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 36cda7c70419a9c2d08cb110dd58b099.
Strike Shiz_3e302468	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 3e30246888275ebb416d4165f71b1fe8.
Strike Shiz_3f751fb4	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 3f751fb44ca9c7117fd90a07b2d32ee9.
Strike Shiz_47de3e4f	This strike sends a polymorphic malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Shiz sample is 47de3e4f669440589fe34532ad9114b2.
Strike Shiz_485acf5b	This strike sends a polymorphic malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The binary has random bytes appended at the end of the file. The MD5 hash of this Shiz sample is 485acf5b5c53e4b6f61c4add87c6373f.

<b>Name</b>	<b>Description</b>
Strike Shiz_49d9cd89	This strike sends a polymorphic malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The binary has random bytes appended at the end of the file. The MD5 hash of this Shiz sample is 49d9cd897d3e7c90623540b51bbc26bc.
Strike Shiz_4bf9fddc	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 4bf9fddcd198b5cf5520bffd78be0c3c.
Strike Shiz_4cc39df1	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 4cc39df1f7950b7883fd861af127afd4.
Strike Shiz_4cc67d26	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 4cc67d2675a6f56f5c225c3eb05514b3.
Strike Shiz_4f199253	This strike sends a polymorphic malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Shiz sample is 4f199253542d306639e414eececcfbfa.
Strike Shiz_54a0c5c0	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 54a0c5c04b7cb0eba0d7614b41569b1b.
Strike Shiz_59a089a2	This strike sends a polymorphic malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The binary has the checksum removed in the PE file format. The MD5 hash of this Shiz sample is 59a089a2c1cab2bd3f9c733cdc4f96cd.
Strike Shiz_59e0ece2	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 59e0ece2c571c1b1869c1e51888087c7.
Strike Shiz_5bc37cdd	This strike sends a polymorphic malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The binary has random bytes appended at the end of the file. The MD5 hash of this Shiz sample is 5bc37cddf1f3be9ad2f6d194a7206879.

<b>Name</b>	<b>Description</b>
Strike Shiz_62c6255f	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 62c6255f31f5d39b369f54f5f95d2edc.
Strike Shiz_6d394aee	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 6d394aeefa7d26f6d519a80138424f09.
Strike Shiz_6d3cbc15	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 6d3cbc15a8831097e04672b19add433f.
Strike Shiz_71115b7a	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 71115b7a8bd924854ee7a48c4b81ec5f.
Strike Shiz_81d65ce1	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 81d65ce15ce7fa9bfb9126d5644520b2.
Strike Shiz_8d53c30c	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 8d53c30c043c6b1a0cd34efa938caaf0.
Strike Shiz_9512be16	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is 9512be161d22bff3834ba5fecdc4eb6.
Strike Shiz_a15fbb32	This strike sends a polymorphic malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Shiz sample is a15fbb32ccf830baf1c4adbc32c871b6.
Strike Shiz_a1bee642	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is a1bee64292749498f62b3b0569fc66d4.
Strike Shiz_a451eb6c	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is a451eb6c5c0310114363df86a61b091b.

<b>Name</b>	<b>Description</b>
Strike Shiz_a47a581f	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is a47a581f94f93bef024f2f9c099ac15e.
Strike Shiz_a4c74c50	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is a4c74c5072de775c8bf23db0fea9e3f6.
Strike Shiz_b521ef3d	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is b521ef3da1cbd0f2883ac45bff7d2f7e.
Strike Shiz_ba522cea	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is ba522ceacf187c3aeee16f32af3031aa4.
Strike Shiz_c7e856bb	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is c7e856bba1e2e1abcecc9757f49c69fd.
Strike Shiz_d072d816	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is d072d816a7fd9b22d226fe4e27289e5a.
Strike Shiz_d1f42be9	This strike sends a polymorphic malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Shiz sample is d1f42be9b1870a1b52cf2dc07ff508e9.
Strike Shiz_d4a279b2	This strike sends a polymorphic malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Shiz sample is d4a279b2c8c86d8434c24de05f041252.
Strike Shiz_d662f757	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is d662f75719f02414a66a17b16a2c721d.

<b>Name</b>	<b>Description</b>
Strike Shiz_e136f6c7	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is e136f6c7b1f2cf7e6454e8dda99ae133.
Strike Shiz_e7e1bd55	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is e7e1bd5531ca3ad87a051bac9d1a80d3.
Strike Shiz_e811ff63	This strike sends a polymorphic malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Shiz sample is e811ff638e5c82869e40fc2a697de1b6.
Strike Shiz_eae062b8	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is eae062b8d75e0d3e442ed62a44a94b73.
Strike Shiz_eb6557c1	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is eb6557c1446859b1c4397535f8d68cb5.
Strike Shiz_eefadc74	This strike sends a malware sample known as Shiz. Shiz is a remote access trojan that allows an attacker to access an infected machine to harvest sensitive information like application passwords and browser cookies. The MD5 hash of this Shiz sample is eefadc749a3d7eb5ffde51f741241115.
Strike Shlayer_04e7bae9	This strike sends a malware sample known as Shlayer. Shlayer is a Trojan family of malware that targets the Mac OS platform. Its main purpose is to infect a system and retrieve additional malware most typically adware. Like most adware, it displays unwanted advertising on the system. Most recently Shlayer has been delivered with Apple notarized applications. The MD5 hash of this Shlayer sample is 04e7bae95f86118fd5e347ee43537b06.
Strike Shlayer_1c859729	This strike sends a malware sample known as Shlayer. Shlayer is a Trojan family of malware that targets the Mac OS platform. Its main purpose is to infect a system and retrieve additional malware most typically adware. Like most adware, it displays unwanted advertising on the system. Most recently Shlayer has been delivered with Apple notarized applications. The MD5 hash of this Shlayer sample is 1c859729bde4b392eaa1694c19ba5f9c.
Strike Shlayer_4d86ae25	This strike sends a malware sample known as Shlayer. Shlayer is a Trojan family of malware that targets the Mac OS platform. Its main purpose is to infect a system and retrieve additional malware most typically adware. Like most adware, it displays unwanted advertising on the system. Most recently Shlayer has been delivered with Apple notarized applications. The MD5 hash of this Shlayer sample is 4d86ae25913374cfcb80a8d798b9016e.

<b>Name</b>	<b>Description</b>
Strike Shlayer_594aa050	This strike sends a malware sample known as Shlayer. Shlayer is a Trojan family of malware that targets the Mac OS platform. Its main purpose is to infect a system and retrieve additional malware most typically adware. Like most adware, it displays unwanted advertising on the system. Most recently Shlayer has been delivered with Apple notarized applications. The MD5 hash of this Shlayer sample is 594aa050742406db04a8e07b5d247cdd.
Strike Shlayer_6ac3ae1c	This strike sends a malware sample known as Shlayer. Shlayer is a Trojan family of malware that targets the Mac OS platform. Its main purpose is to infect a system and retrieve additional malware most typically adware. Like most adware, it displays unwanted advertising on the system. Most recently Shlayer has been delivered with Apple notarized applications. The MD5 hash of this Shlayer sample is 6ac3ae1ccb9038388e492a64ef08e5ec.
Strike Shlayer_9c88732f	This strike sends a malware sample known as Shlayer. Shlayer is a Trojan family of malware that targets the Mac OS platform. Its main purpose is to infect a system and retrieve additional malware most typically adware. Like most adware, it displays unwanted advertising on the system. Most recently Shlayer has been delivered with Apple notarized applications. The MD5 hash of this Shlayer sample is 9c88732f4a04c10ec4853f871de6b5eb.
Strike Shlayer_b2b51960	This strike sends a malware sample known as Shlayer. Shlayer is a Trojan family of malware that targets the Mac OS platform. Its main purpose is to infect a system and retrieve additional malware most typically adware. Like most adware, it displays unwanted advertising on the system. Most recently Shlayer has been delivered with Apple notarized applications. The MD5 hash of this Shlayer sample is b2b519602673e27aa40085deb8827bd1.
Strike Shlayer_c4e8f038	This strike sends a malware sample known as Shlayer. Shlayer is a Trojan family of malware that targets the Mac OS platform. Its main purpose is to infect a system and retrieve additional malware most typically adware. Like most adware, it displays unwanted advertising on the system. Most recently Shlayer has been delivered with Apple notarized applications. The MD5 hash of this Shlayer sample is c4e8f03892756086e9813db09485b0bc.
Strike Shlayer_e8a9e861	This strike sends a malware sample known as Shlayer. Shlayer is a Trojan family of malware that targets the Mac OS platform. Its main purpose is to infect a system and retrieve additional malware most typically adware. Like most adware, it displays unwanted advertising on the system. Most recently Shlayer has been delivered with Apple notarized applications. The MD5 hash of this Shlayer sample is e8a9e8617f6f83729e5c4bec46ad1c77.
Strike Shlayer_fa124ed3	This strike sends a malware sample known as Shlayer. Shlayer is a Trojan family of malware that targets the Mac OS platform. Its main purpose is to infect a system and retrieve additional malware most typically adware. Like most adware, it displays unwanted advertising on the system. Most recently Shlayer has been delivered with Apple notarized applications. The MD5 hash of this Shlayer sample is fa124ed3905a9075517f497531779f92.
Strike Shlayer_fefcf50	This strike sends a malware sample known as Shlayer. Shlayer is a Trojan family of malware that targets the Mac OS platform. Its main purpose is to infect a system and retrieve additional malware most typically adware. Like most adware, it displays unwanted advertising on the system. Most recently Shlayer has been delivered with Apple notarized applications. The MD5 hash of this Shlayer sample is fefcf50214786bbbd33ee67abd7f1f3.

<b>Name</b>	<b>Description</b>
Strike Sidewinder_0aea0695	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 0aea06959cdd43e43f8b9d4625267398.
Strike Sidewinder_243bfa39	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 243bfa3990d9b263e6ac1265735f79be.
Strike Sidewinder_6dbc9a6f	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 6dbc9a6f81f99e7c32529ab9835cbcfc0.
Strike Sidewinder_81dfbdb2	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 81dfbdb2056db1b33440e8d3d57511d5.
Strike Sidewinder_88109f66	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 88109f669191ff1809c662a6691dcfc7.

<b>Name</b>	<b>Description</b>
Strike Sidewinder_888b6313	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 888b6313812112cae5c16d2e39a74d30.
Strike Sidewinder_99c545ba	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 99c545ba0a638a1ccd48e72372ea4e88.
Strike Sidewinder_9e10fea1	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is 9e10fea142ce2fbc729f2bb30178ba79.
Strike Sidewinder_b8819140	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is b881914069d0dbbedd70cd8319541d7c.
Strike Sidewinder_d2b300dc	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is d2b300dce04690bc227cd7e7f0bb07a9.

<b>Name</b>	<b>Description</b>
Strike Sidewinder_e567f387	This strike sends a malware sample known as Sidewinder. Sidewinder APT is a malware group that uses a variety of lures, decoy documents, and applications to infiltrate their targets. It uses a .NET-based malware called SharpStage and a document stealer called BlatSting. Upon execution, SharpStage downloads additional payloads and BlatSting steals documents. Key capabilities of the malware include downloading and executing additional payloads, stealing documents, and evading detection by using legitimate Windows features and obfuscated code. The MD5 hash of this Sidewinder sample is e567f3877e3a206d31629409ed7e1910.
Strike SlowStepper_2ba80036	This strike sends a malware sample known as SlowStepper. SlowStepper is a backdoor malware. This malware is associated with the PlushDaemon Chinese APT group that hijacks legitimate applications and redirects victims to attacker controlled servers. This sample is tied to a trojanized version of the IPany VPN software. The MD5 hash of this SlowStepper sample is 2ba80036b9554d9722e199e9d0065831.
Strike SlowStepper_e2bc2361	This strike sends a malware sample known as SlowStepper. SlowStepper is a backdoor malware. This malware is associated with the PlushDaemon Chinese APT group that hijacks legitimate applications and redirects victims to attacker controlled servers. This sample is tied to a trojanized version of the IPany VPN software. The MD5 hash of this SlowStepper sample is e2bc2361ead7c80eba86a5d1c492865d.
Strike SlowStepper_ecb6b71b	This strike sends a malware sample known as SlowStepper. SlowStepper is a backdoor malware. This malware is associated with the PlushDaemon Chinese APT group that hijacks legitimate applications and redirects victims to attacker controlled servers. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this SlowStepper sample is ecb6b71bf815f5509629ee028887b3dd.
Strike SnappyBee_334c9477	This strike sends a malware sample known as SnappyBee. SnappyBee is a modular backdoor malware. Recently it has been associated with Earth E strikes aka Salt Typhoon campaigns. The malware is typically launched as a follow on backdoor via DLL sideloading techniques. The MD5 hash of this SnappyBee sample is 334c9477f71802c57349a997b8bf6d61.
Strike SnappyBee_43f3f328	This strike sends a malware sample known as SnappyBee. SnappyBee is a modular backdoor malware. Recently it has been associated with Earth E strikes aka Salt Typhoon campaigns. The malware is typically launched as a follow on backdoor via DLL sideloading techniques. The MD5 hash of this SnappyBee sample is 43f3f328248da7bda95407968604ff0b.
Strike SnappyBee_45d79973	This strike sends a malware sample known as SnappyBee. SnappyBee is a modular backdoor malware. Recently it has been associated with Earth E strikes aka Salt Typhoon campaigns. The malware is typically launched as a follow on backdoor via DLL sideloading techniques. The MD5 hash of this SnappyBee sample is 45d7997340065904ae092ac427c54f41.
Strike SnappyBee_505b55c2	This strike sends a malware sample known as SnappyBee. SnappyBee is a modular backdoor malware. Recently it has been associated with Earth E strikes aka Salt Typhoon campaigns. The malware is typically launched as a follow on backdoor via DLL sideloading techniques. The MD5 hash of this SnappyBee sample is 505b55c2b68e32acb5ad13588e1491a5.

<b>Name</b>	<b>Description</b>
Strike SnappyBee_8bd8506f	This strike sends a malware sample known as SnappyBee. SnappyBee is a modular backdoor malware. Recently it has been associated with Earth E strikes aka Salt Typhoon campaigns. The malware is typically launched as a follow on backdoor via DLL sideloading techniques. The MD5 hash of this SnappyBee sample is 8bd8506f6b1a80eea68e877fa81e267c.
Strike SnappyBee_b706f480	This strike sends a malware sample known as SnappyBee. SnappyBee is a modular backdoor malware. Recently it has been associated with Earth E strikes aka Salt Typhoon campaigns. The malware is typically launched as a follow on backdoor via DLL sideloading techniques. The MD5 hash of this SnappyBee sample is b706f4806dc88611873caddeb3ad1ff97.
Strike SnipBot_0cd8736a	This strike sends a malware sample known as SnipBot. SnipBot is malware that is being associated with the RomCom malware family. The malware is usually composed of several stages. It begins with some sort of phishing attempt, typically a pdf document that initiates the infection process and delivers a signed executable. This malware has RAT functionality, and gives attackers the ability to execute commands and download modules onto a victim's system. The MD5 hash of this SnipBot sample is 0cd8736a915e8e32ddeda21ed462670b.
Strike SnipBot_36d4903f	This strike sends a malware sample known as SnipBot. SnipBot is malware that is being associated with the RomCom malware family. The malware is usually composed of several stages. It begins with some sort of phishing attempt, typically a pdf document that initiates the infection process and delivers a signed executable. This malware has RAT functionality, and gives attackers the ability to execute commands and download modules onto a victim's system. The MD5 hash of this SnipBot sample is 36d4903ffafa75c00460292881b5dad7.
Strike SnipBot_43cc1f2f	This strike sends a malware sample known as SnipBot. SnipBot is malware that is being associated with the RomCom malware family. The malware is usually composed of several stages. It begins with some sort of phishing attempt, typically a pdf document that initiates the infection process and delivers a signed executable. This malware has RAT functionality, and gives attackers the ability to execute commands and download modules onto a victim's system. The MD5 hash of this SnipBot sample is 43cc1f2f07c1c1c7f69075d81332f95e.
Strike SnipBot_524dda24	This strike sends a malware sample known as SnipBot. SnipBot is malware that is being associated with the RomCom malware family. The malware is usually composed of several stages. It begins with some sort of phishing attempt, typically a pdf document that initiates the infection process and delivers a signed executable. This malware has RAT functionality, and gives attackers the ability to execute commands and download modules onto a victim's system. The MD5 hash of this SnipBot sample is 524dda2410cc7ee8cc326ca42cebd7dd.
Strike SnipBot_6fa6dd33	This strike sends a malware sample known as SnipBot. SnipBot is malware that is being associated with the RomCom malware family. The malware is usually composed of several stages. It begins with some sort of phishing attempt, typically a pdf document that initiates the infection process and delivers a signed executable. This malware has RAT functionality, and gives attackers the ability to execute commands and download modules onto a victim's system. The MD5 hash of this SnipBot sample is 6fa6dd331844ee5cfe20c74353c1e442.

<b>Name</b>	<b>Description</b>
Strike SnipBot_7f2e4a44	This strike sends a malware sample known as SnipBot. SnipBot is malware that is being associated with the RomCom malware family. The malware is usually composed of several stages. It begins with some sort of phishing attempt, typically a pdf document that initiates the infection process and delivers a signed executable. This malware has RAT functionality, and gives attackers the ability to execute commands and download modules onto a victim's system. The MD5 hash of this SnipBot sample is 7f2e4a44445b977ef8917cc0fb79035b.
Strike SnipBot_c0e49940	This strike sends a malware sample known as SnipBot. SnipBot is malware that is being associated with the RomCom malware family. The malware is usually composed of several stages. It begins with some sort of phishing attempt, typically a pdf document that initiates the infection process and delivers a signed executable. This malware has RAT functionality, and gives attackers the ability to execute commands and download modules onto a victim's system. The MD5 hash of this SnipBot sample is c0e499402acb6c302228b4a7923d5db6.
Strike SnipBot_d69cf309	This strike sends a malware sample known as SnipBot. SnipBot is malware that is being associated with the RomCom malware family. The malware is usually composed of several stages. It begins with some sort of phishing attempt, typically a pdf document that initiates the infection process and delivers a signed executable. This malware has RAT functionality, and gives attackers the ability to execute commands and download modules onto a victim's system. The MD5 hash of this SnipBot sample is d69cf309cb0e5d91237c6454e0e0dc45.
Strike SnipBot_fa400cb7	This strike sends a malware sample known as SnipBot. SnipBot is malware that is being associated with the RomCom malware family. The malware is usually composed of several stages. It begins with some sort of phishing attempt, typically a pdf document that initiates the infection process and delivers a signed executable. This malware has RAT functionality, and gives attackers the ability to execute commands and download modules onto a victim's system. The MD5 hash of this SnipBot sample is fa400cb70d13cb329d05877b8fe73ed5.
Strike Sodinokibi_177a571d	This strike sends a malware sample known as Sodinokibi. Sodinokibi ransomware takes advantage of a Oracle WebLogic vulnerability to gain access to target system. Once inside, it attempts to elevate privileges in order to access all files and resources on the system without any restriction. It will then wipe out all files in the backup folder. The MD5 hash of this Sodinokibi sample is 177a571d7c6a6e4592c60a78b574fe0e.
Strike Sodinokibi_858c29ef	This strike sends a polymorphic malware sample known as Sodinokibi. Sodinokibi ransomware takes advantage of a Oracle WebLogic vulnerability to gain access to target system. Once inside, it attempts to elevate privileges in order to access all files and resources on the system without any restriction. It will then wipe out all files in the backup folder. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Sodinokibi sample is 858c29efee084e86616b21fdc4d2a3de.

<b>Name</b>	<b>Description</b>
Strike Sodinokibi_bf935904	This strike sends a malware sample known as Sodinokibi. Sodinokibi ransomware takes advantage of a Oracle WebLogic vulnerability to gain access to target system. Once inside, it attempts to elevate privileges in order to access all files and resources on the system without any restriction. It will then wipe out all files in the backup folder. The MD5 hash of this Sodinokibi sample is bf9359046c4f5c24de0a9de28bbabd14.
Strike Sodinokibi_e713658b	This strike sends a malware sample known as Sodinokibi. Sodinokibi ransomware takes advantage of a Oracle WebLogic vulnerability to gain access to target system. Once inside, it attempts to elevate privileges in order to access all files and resources on the system without any restriction. It will then wipe out all files in the backup folder. The MD5 hash of this Sodinokibi sample is e713658b666ff04c9863ebecb458f174.
Strike Sodinokibi_fb68a023	This strike sends a malware sample known as Sodinokibi. Sodinokibi ransomware takes advantage of a Oracle WebLogic vulnerability to gain access to target system. Once inside, it attempts to elevate privileges in order to access all files and resources on the system without any restriction. It will then wipe out all files in the backup folder. The MD5 hash of this Sodinokibi sample is fb68a02333431394a9a0cdbff3717b24.
Strike SolarPhantom_0700af85	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 0700af859d2379420774145592f8862e.
Strike SolarPhantom_1a5e7b4c	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 1a5e7b4cbe34ee385225da8715562f5d.

<b>Name</b>	<b>Description</b>
Strike SolarPhantom_1adbaaa3	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 1adbaaa352a8366c03faaa44fc5d4687.
Strike SolarPhantom_23807082	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 23807082358d736404cf935fe7c65b5.
Strike SolarPhantom_38cbe65f	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 38cbe65f8d2221a6c1b32abd4c96206d.
Strike SolarPhantom_50b9e707	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 50b9e707bd2c1adff933a688ee862463.

<b>Name</b>	<b>Description</b>
Strike SolarPhantom_55419e51	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 55419e51ef8a0521f5d7075dbec7bc33.</p>
Strike SolarPhantom_59f1bbdc	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 59f1bbdc298a9c8a39ec393caf6ceef5.</p>
Strike SolarPhantom_653eb0de	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 653eb0de6c8d12eb40b76b59500a06c2.</p>
Strike SolarPhantom_682e7926	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 682e79264e8e7bde1e224a3c13492d50.</p>

<b>Name</b>	<b>Description</b>
Strike SolarPhantom_6fad60bf	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 6fad60bfc2d7e2b0781618467af045a9.</p>
Strike SolarPhantom_6fc09961	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 6fc09961ed82caa2e23f6efe820ca0cb.</p>
Strike SolarPhantom_7984837e	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 7984837e254f860a29b7a4d811a25963.</p>
Strike SolarPhantom_7d21a0c4	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 7d21a0c42e51f0fa9324cde55252be27.</p>

<b>Name</b>	<b>Description</b>
Strike SolarPhantom_7d8c0e47	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 7d8c0e47d88dc6dbfa82793803a2bcf5.</p>
Strike SolarPhantom_806bad0e	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 806bad0e26b540bc31b1d566531b95fa.</p>
Strike SolarPhantom_80b2e25a	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 80b2e25abd8a70909cc7b94bec90efc2.</p>
Strike SolarPhantom_848af416	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 848af416d94bb62257df869c54e1c13f.</p>

<b>Name</b>	<b>Description</b>
Strike SolarPhantom_9413444e	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 9413444e0ed67798d044acdcb2b9a4f8.
Strike SolarPhantom_9b5c28bf	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is 9b5c28bfce74a166e764a996f60bef15.
Strike SolarPhantom_afecc46a	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is afecc46a346af09f5a9b4c7739986a8d.
Strike SolarPhantom_b3447a64	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is b3447a648b588d2fc40cdd5b3eb7542e.

<b>Name</b>	<b>Description</b>
Strike SolarPhantom_b62aa586	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is b62aa5869c43fdbd9995aed9ec33ce41b.
Strike SolarPhantom_b8979951	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is b897995143105e5255500341ae48bc9b.
Strike SolarPhantom_bf55a651	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is bf55a651364edeb64f2e37ff86a094b8.
Strike SolarPhantom_c37e3172	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is c37e317293b94c933ebaa6410ba85aaa.

<b>Name</b>	<b>Description</b>
Strike SolarPhantom_d3274945	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is d327494547be8cb70479358517f47b1e.</p>
Strike SolarPhantom_e33c50ee	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is e33c50ee3bdb341ae0739c9b0a1093c1.</p>
Strike SolarPhantom_e4d1337f	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is e4d1337fdb8bc461a656ed6405184f5e.</p>
Strike SolarPhantom_ecc294c1	<p>This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is ecc294c108e6efe26952b0f1278e6c68.</p>

Name	Description
Strike SolarPhantom_ee6b67ed	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is ee6b67ed7b062cd1a34bcee528b574dd.
Strike SolarPhantom_f5321b32	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is f5321b32e719e876feae3b5e4a875377.
Strike SolarPhantom_fbb0b7d9	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is fbb0b7d940a7ad6a7187eed00f6870b5.
Strike SolarPhantom_fea30627	This strike sends a malware sample known as SolarPhantom. SolarPhantom is an advanced malware linked to the SolarMarker threat actor, primarily in .NET with a Delphi-coded hVNC backdoor. It targets diverse industries through compromised WordPress sites and manipulates browser processes. Its hVNC functionality captures webcam footage and simulates mouse events on a hidden virtual desktop. The malware employs evasion techniques, disabling browser metrics and hardware acceleration. During execution, it communicates with the C2 server, sending host computer details and a randomly generated HWID. SolarPhantom showcases adaptability, modifying its PowerShell script and employing varying delivery methods and payloads. The MD5 hash of this SolarPhantom sample is fea30627a4cdb82aaaf9d0d7a47b46115.

Name	Description
Strike SpyBanker_5b1203a0	<p>This strike sends a malware sample known as SpyBanker. The malware disguises itself as official banking apps, employing a common social engineering tactic to impersonate legitimate banks and financial institution that targets customers of major financial institutions. The campaigns involve sharing malicious APK files through platforms like WhatsApp, prompting users to enter sensitive information. The installed fraudulent app impersonates a legitimate Indian bank's Know Your Customer (KYC) application, tricking users into submitting sensitive information, which is then sent to a command and control (C2) server and the attacker's designated phone number. 'com.sk.axisbank' is the package name of the malware sample. The MD5 hash of this malware sample is 5b1203a0def70d1f5aff2bf67d7c9537.</p>
Strike SpyBanker_63689e7c	<p>This strike sends a polymorphic malware sample known as SpyBanker. The malware disguises itself as official banking apps, employing a common social engineering tactic to impersonate legitimate banks and financial institution that targets customers of major financial institutions. The campaigns involve sharing malicious APK files through platforms like WhatsApp, prompting users to enter sensitive information. The installed fraudulent app impersonates a legitimate Indian bank's Know Your Customer (KYC) application, tricking users into submitting sensitive information, which is then sent to a command and control (C2) server and the attacker's designated phone number. 'com.sk.axisbank' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 63689e7c7e32815fb1d8133d2c5525fa.</p>
Strike SpyBanker_e5701b03	<p>This strike sends a polymorphic malware sample known as SpyBanker. The malware disguises itself as official banking apps, employing a common social engineering tactic to impersonate legitimate banks and financial institution that targets customers of major financial institutions. The campaigns involve sharing malicious APK files through platforms like WhatsApp, prompting users to enter sensitive information. The installed fraudulent app impersonates a legitimate Indian bank's Know Your Customer (KYC) application, tricking users into submitting sensitive information, which is then sent to a command and control (C2) server and the attacker's designated phone number. 'com.sk.axisbank' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is e5701b03a53fc0613fd94b5a7d233236.</p>
Strike SpyBanker_e6c33ffa	<p>This strike sends a polymorphic malware sample known as SpyBanker. The malware disguises itself as official banking apps, employing a common social engineering tactic to impersonate legitimate banks and financial institution that targets customers of major financial institutions. The campaigns involve sharing malicious APK files through platforms like WhatsApp, prompting users to enter sensitive information. The installed fraudulent app impersonates a legitimate Indian bank's Know Your Customer (KYC) application, tricking users into submitting sensitive information, which is then sent to a command and control (C2) server and the attacker's designated phone number. 'com.sk.axisbank' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is e6c33ffabf6c22c8c42d0c522bbd3fcc.</p>

<b>Name</b>	<b>Description</b>
Strike SpyLoan_3461f57f	<p>This strike sends a polymorphic malware sample known as SpyLoan. The malware masquerades as Android loan apps, presenting itself as a financial service while actively collecting personal and financial data. The apps, distributed through social media, SMS, and scam websites, employ coercive practices, harassing users even when loans are not granted. The operators, primarily from various countries, coerce victims into providing extensive permissions during installation, thereby granting access to sensitive information. The apps demand personal details, including contact information, proof of income, and banking information, along with collecting additional device data. The harvested information is then actively exfiltrated to a command-and-control server using encryption techniques. 'com.app.lo.go' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 3461f57f0fa50a5f8c5d6b1208181351.</p>
Strike SpyLoan_4f1c2ebb	<p>This strike sends a malware sample known as SpyLoan. The malware masquerades as Android loan apps, presenting itself as a financial service while actively collecting personal and financial data. The apps, distributed through social media, SMS, and scam websites, employ coercive practices, harassing users even when loans are not granted. The operators, primarily from various countries, coerce victims into providing extensive permissions during installation, thereby granting access to sensitive information. The apps demand personal details, including contact information, proof of income, and banking information, along with collecting additional device data. The harvested information is then actively exfiltrated to a command-and-control server using encryption techniques. 'com.mlo.xango' is the package name of the malware sample. The MD5 hash of this malware sample is 4f1c2ebb125017b1a13a51ea941f7bc1.</p>
Strike SpyLoan_5579637d	<p>This strike sends a polymorphic malware sample known as SpyLoan. The malware masquerades as Android loan apps, presenting itself as a financial service while actively collecting personal and financial data. The apps, distributed through social media, SMS, and scam websites, employ coercive practices, harassing users even when loans are not granted. The operators, primarily from various countries, coerce victims into providing extensive permissions during installation, thereby granting access to sensitive information. The apps demand personal details, including contact information, proof of income, and banking information, along with collecting additional device data. The harvested information is then actively exfiltrated to a command-and-control server using encryption techniques. 'com.mlo.xango' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 5579637d174bd99502b43830a17fac93.</p>
Strike SpyLoan_88e1f702	<p>This strike sends a polymorphic malware sample known as SpyLoan. The malware masquerades as Android loan apps, presenting itself as a financial service while actively collecting personal and financial data. The apps, distributed through social media, SMS, and scam websites, employ coercive practices, harassing users even when loans are not granted. The operators, primarily from various countries, coerce victims into providing extensive permissions during installation, thereby granting access to sensitive information. The apps demand personal details, including contact information, proof of income, and banking information, along with collecting additional device data. The harvested information is then actively exfiltrated to a command-and-control server using encryption techniques. 'com.mlo.xango' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 88e1f7020afb5ea845f1d4c4c41d3542.</p>

<b>Name</b>	<b>Description</b>
Strike SpyLoan_a2732894	<p>This strike sends a polymorphic malware sample known as SpyLoan. The malware masquerades as Android loan apps, presenting itself as a financial service while actively collecting personal and financial data. The apps, distributed through social media, SMS, and scam websites, employ coercive practices, harassing users even when loans are not granted. The operators, primarily from various countries, coerce victims into providing extensive permissions during installation, thereby granting access to sensitive information. The apps demand personal details, including contact information, proof of income, and banking information, along with collecting additional device data. The harvested information is then actively exfiltrated to a command-and-control server using encryption techniques. 'com.mlo.xango' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is a2732894106e353465e7b257478aca7e.</p>
Strike SpyLoan_a4b83ae2	<p>This strike sends a polymorphic malware sample known as SpyLoan. The malware masquerades as Android loan apps, presenting itself as a financial service while actively collecting personal and financial data. The apps, distributed through social media, SMS, and scam websites, employ coercive practices, harassing users even when loans are not granted. The operators, primarily from various countries, coerce victims into providing extensive permissions during installation, thereby granting access to sensitive information. The apps demand personal details, including contact information, proof of income, and banking information, along with collecting additional device data. The harvested information is then actively exfiltrated to a command-and-control server using encryption techniques. 'com.app.lo.go' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is a4b83ae23ccd959f8244060783982bfa.</p>
Strike SpyLoan_cd15f394	<p>This strike sends a polymorphic malware sample known as SpyLoan. The malware masquerades as Android loan apps, presenting itself as a financial service while actively collecting personal and financial data. The apps, distributed through social media, SMS, and scam websites, employ coercive practices, harassing users even when loans are not granted. The operators, primarily from various countries, coerce victims into providing extensive permissions during installation, thereby granting access to sensitive information. The apps demand personal details, including contact information, proof of income, and banking information, along with collecting additional device data. The harvested information is then actively exfiltrated to a command-and-control server using encryption techniques. 'com.app.lo.go' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is cd15f3942f10893b81e79d922b96e091.</p>
Strike SpyLoan_da1580cb	<p>This strike sends a malware sample known as SpyLoan. The malware masquerades as Android loan apps, presenting itself as a financial service while actively collecting personal and financial data. The apps, distributed through social media, SMS, and scam websites, employ coercive practices, harassing users even when loans are not granted. The operators, primarily from various countries, coerce victims into providing extensive permissions during installation, thereby granting access to sensitive information. The apps demand personal details, including contact information, proof of income, and banking information, along with collecting additional device data. The harvested information is then actively exfiltrated to a command-and-control server using encryption techniques. 'com.app.lo.go' is the package name of the malware sample. The MD5 hash of this malware sample is da1580cb6f79c758c4079f16eb9b50fe.</p>

<b>Name</b>	<b>Description</b>
Strike SpyNote_426e3883	This strike sends a polymorphic malware sample known as SpyNote RAT. SpyNote is a stealthy Android malware that spreads through phishing campaigns, including smishing and fake online alerts. SpyNote uses the Accessibility API to target famous crypto wallets. Masquerading as legitimate applications, SpyNote steals sensitive information like messages, contacts, and keystrokes. Recent versions have started targeting banking apps, which makes it even more dangerous. SpyNote hides its activity and is difficult to remove. 'com.shriram' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 426e3883d8409cccaafde2ce44a59057.
Strike SpyNote_5cb3105f	This strike sends a polymorphic malware sample known as SpyNote RAT. SpyNote is a stealthy Android malware that spreads through phishing campaigns, including smishing and fake online alerts. SpyNote uses the Accessibility API to target famous crypto wallets. Masquerading as legitimate applications, SpyNote steals sensitive information like messages, contacts, and keystrokes. Recent versions have started targeting banking apps, which makes it even more dangerous. SpyNote hides its activity and is difficult to remove. 'com.shriram' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 5cb3105f8623b44927d23daabb9d2b71.
Strike SpyNote_fd2750e3	This strike sends a malware sample known as SpyNote RAT. SpyNote is a stealthy Android malware that spreads through phishing campaigns, including smishing and fake online alerts. SpyNote uses the Accessibility API to target famous crypto wallets. Masquerading as legitimate applications, SpyNote steals sensitive information like messages, contacts, and keystrokes. Recent versions have started targeting banking apps, which makes it even more dangerous. SpyNote hides its activity and is difficult to remove. 'com.shriram' is the package name of the malware sample. The MD5 hash of this malware sample is fd2750e3be8c5ad625bedbebfaa8f03b.
Strike Spynote-ChatGPT_3a882f8a	This strike sends an Android polymorphic malware sample known as Spynote. The particular sample poses as a ChatGPT like app named AI Photo. It's a spyware which steals sensitive data such as call logs, contacts, SMSs, media files, and other data from an infected device. 'cmf0.c3b5bm90zq.patch' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this Spynote sample is 3a882f8a05e9455d6c0fe389b15874cc.
Strike Spynote-ChatGPT_62130fe4	This strike sends an Android polymorphic malware sample known as Spynote. The particular sample poses as a ChatGPT like app named AI Photo. It's a spyware which steals sensitive data such as call logs, contacts, SMSs, media files, and other data from an infected device. 'cmf0.c3b5bm90zq.patch' is the package name of the malware sample. The malware has been randomly rebuilt without any modifications. The MD5 hash of this Spynote sample is 62130fe4f725fe9e3d0d6d12fcfd2711e.
Strike Spynote-ChatGPT_8468af0e	This strike sends an Android malware sample known as Spynote. The particular sample poses as a ChatGPT like app named AI Photo. It's a spyware which steals sensitive data such as call logs, contacts, SMSs, media files, and other data from an infected device. 'cmf0.c3b5bm90zq.patch' is the package name of the malware sample. The MD5 hash of this Spynote sample is 174539797080a9bcbb3f32c5865700bf.

<b>Name</b>	<b>Description</b>
Strike Stealc_0d049f76	This strike sends a malware sample known as Stealc. The Stealc malware is a Malware-As-A-Service Info stealer that relies on Vidar raccoon and redline stealers. It steals sensitive data from web browsers, browser extensions for cryptocurrency wallets, desktop cryptocurrency wallets as well as email client and messenger information. It allows the customers to configure the options on how to grab files from the victim machine. The MD5 hash of this Stealc sample is 0d049f764a22e16933f8c3f1704d4e50.
Strike Stealc_7b9cc53b	This strike sends a malware sample known as Stealc. The Stealc malware is a Malware-As-A-Service Info stealer that relies on Vidar raccoon and redline stealers. It steals sensitive data from web browsers, browser extensions for cryptocurrency wallets, desktop cryptocurrency wallets as well as email client and messenger information. It allows the customers to configure the options on how to grab files from the victim machine. The MD5 hash of this Stealc sample is 7b9cc53b66d07dfa782f75ffa5e503fe.
Strike Stealc_9f1aae2b	This strike sends a malware sample known as Stealc. The Stealc malware is a Malware-As-A-Service Info stealer that relies on Vidar raccoon and redline stealers. It steals sensitive data from web browsers, browser extensions for cryptocurrency wallets, desktop cryptocurrency wallets as well as email client and messenger information. It allows the customers to configure the options on how to grab files from the victim machine. The MD5 hash of this Stealc sample is 9f1aae2b56ebe6681de5d6a376394e29.
Strike Storm-0324_0fa25c37	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is 0fa25c37597f430d14f20b3a503b6fdb.
Strike Storm-0324_43571622	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is 435716225798149de4277ec910d6ca51.
Strike Storm-0324_60250264	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is 602502641978f786d4ef8a1f25de314d.

<b>Name</b>	<b>Description</b>
Strike Storm-0324_70bf088f	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is 70bf088f2815a61ad2b1cc9d6e119a7f.
Strike Storm-0324_739607a0	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is 739607a0ab5388fb9714da17e7affce8.
Strike Storm-0324_7e36870f	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is 7e36870fa5d1e33d77a5d0b69b46a090.
Strike Storm-0324_8052c7fa	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is 8052c7fa20ede77f6d6777015e926242.
Strike Storm-0324_98552ccf	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is 98552ccfe01a922ca33cbf3ef58c810b.

<b>Name</b>	<b>Description</b>
Strike Storm-0324_a3892280	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is a3892280be014691dcbab8d5a3227f20.
Strike Storm-0324_a843c701	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is a843c7018c53659ca0293d4d48577209.
Strike Storm-0324_c9d85102	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is c9d85102b3aa7cb9274166b058b2e4fb.
Strike Storm-0324_d80feb14	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is d80feb14c5beebd1c3091ed9f67c4071.
Strike Storm-0324_e0e19b74	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is e0e19b748cbe5fd50a5288ec4b29f024.

<b>Name</b>	<b>Description</b>
Strike Storm-0324_e9a432f5	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is e9a432f52ba21638a40399c76b681e11.
Strike Storm-0324_f459722c	This strike sends a malware sample known as Storm-0324. This sample is related to Storm-0324 which is a financially motivated threat actor group which is known for using email-based phishing campaigns to gain initial access to victim networks, and then selling that access to other threat actors, including ransomware groups. The malwares send phishing email invoice themes such as DocuSign, Quickbooks, and the user is redirected to the SharePoint site where the compressed WSF (Windows Script File)/JS delivers a malicious .Net payload JSSLoader. The MD5 hash of this Storm-0324 sample is f459722c272e4637a0b965fa4c769b16.
Strike Sunburst_2c4a910a	This strike sends a malware sample known as Sunburst. Sunburst is a malware Trojan that has recently attacked many high profile government, technology, telecom, and consulting companies in numerous locations in North America, Asia, Europe, and the Middle East. It is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that allows for it to communicate with external servers to perform Command and Control functionality. The malware lays dormant for an extended period of time and then executes commands, that allow for the transfer and execution of files, profiling the system, and disabling services. The MD5 hash of this Sunburst sample is 2c4a910a1299cdæ2a4e55988a2f102e.
Strike Sunburst_56ceb6d0	This strike sends a malware sample known as Sunburst. Sunburst is a malware Trojan that has recently attacked many high profile government, technology, telecom, and consulting companies in numerous locations in North America, Asia, Europe, and the Middle East. It is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that allows for it to communicate with external servers to perform Command and Control functionality. The malware lays dormant for an extended period of time and then executes commands, that allow for the transfer and execution of files, profiling the system, and disabling services. The MD5 hash of this Sunburst sample is 56ceb6d0011d87b6e4d7023d7ef85676.
Strike Sunburst_731d724e	This strike sends a malware sample known as Sunburst. Sunburst is a malware Trojan that has recently attacked many high profile government, consulting, telecom, and consulting companies in numerous locations in North America, Asia, Europe, and the Middle East. It is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that allows for it to communicate with external servers to perform Command and Control functionality. The malware lays dormant for an extended period of time and then executes commands, that allow for the transfer and execution of files, profiling the system, and disabling services. The MD5 hash of this Sunburst sample is 731d724e8859ef063c03a8b1ab7f81ec.

Name	Description
Strike Sunburst_846e27a6	This strike sends a malware sample known as Sunburst. Sunburst is a malware Trojan that has recently attacked many high profile government, technology, telecom, and consulting companies in numerous locations in North America, Asia, Europe, and the Middle East. It is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that allows for it to communicate with external servers to perform Command and Control functionality. The malware lays dormant for an extended period of time and then executes commands, that allow for the transfer and execution of files, profiling the system, and disabling services. The MD5 hash of this Sunburst sample is 846e27a652a5e1bfbd0ddd38a16dc865.
Strike Sunburst_b91ce2fa	This strike sends a malware sample known as Sunburst. Sunburst is a malware Trojan that has recently attacked many high profile government, technology, telecom, and consulting companies in numerous locations in North America, Asia, Europe, and the Middle East. It is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that allows for it to communicate with external servers to perform Command and Control functionality. The malware lays dormant for an extended period of time and then executes commands, that allow for the transfer and execution of files, profiling the system, and disabling services. The MD5 hash of this Sunburst sample is b91ce2fa41029f6955bff20079468448.
Strike Sunburst_d5aad0d2	This strike sends a malware sample known as Sunburst. Sunburst is a malware Trojan that has recently attacked many high profile government, technology, telecom, and consulting companies in numerous locations in North America, Asia, Europe, and the Middle East. It is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that allows for it to communicate with external servers to perform Command and Control functionality. The malware lays dormant for an extended period of time and then executes commands, that allow for the transfer and execution of files, profiling the system, and disabling services. The MD5 hash of this Sunburst sample is d5aad0d248c237360cf39c054b654d69.
Strike Sunburst_f6d07f3d	This strike sends a malware sample known as Sunburst. Sunburst is a malware Trojan that has recently attacked many high profile government, consulting, telecom, and consulting companies in numerous locations in North America, Asia, Europe, and the Middle East. It is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that allows for it to communicate with external servers to perform Command and Control functionality. The malware lays dormant for an extended period of time and then executes commands, that allow for the transfer and execution of files, profiling the system, and disabling services. The MD5 hash of this Sunburst sample is f6d07f3d81dcea99b27462d100414917.
Strike SuperBear_26893a46	This strike sends a malware sample known as SuperBear. SuperBear is a RAT malware. This RAT exfiltrates system data and communicates with C2 servers to run remote commands like downloading and executing dlls. The MD5 hash of this SuperBear sample is 26893a46de61332fd08820d5dc56cd19.
Strike SuperBear_e49aaa9a	This strike sends a malware sample known as SuperBear. SuperBear is a RAT malware. This RAT exfiltrates system data and communicates with C2 servers to run remote commands like downloading and executing dlls. The MD5 hash of this SuperBear sample is e49aaa9a5933c48feca39f3080a7b94d.

<b>Name</b>	<b>Description</b>
Strike Swisyn_0bbf4eeb	This strike sends a malware sample known as Swisyn. Swisyn is a loader that installs malicious software on the system, including remote access tool functionality, allowing the controller to perform any malicious action. The MD5 hash of this Swisyn sample is 0bbf4eeb3156b94827c8aecff920cf4e.
Strike Swisyn_25a9aeb7	This strike sends a malware sample known as Swisyn. Swisyn is a loader that installs malicious software on the system, including remote access tool functionality, allowing the controller to perform any malicious action. The MD5 hash of this Swisyn sample is 25a9aeb787c07a0e6a664bf3d40bf5da.
Strike Swisyn_5dbec059	This strike sends a malware sample known as Swisyn. Swisyn is a loader that installs malicious software on the system, including remote access tool functionality, allowing the controller to perform any malicious action. The MD5 hash of this Swisyn sample is 5dbec059892d83ce640453b4696187eb.
Strike Swisyn_6949648f	This strike sends a malware sample known as Swisyn. Swisyn is a loader that installs malicious software on the system, including remote access tool functionality, allowing the controller to perform any malicious action. The MD5 hash of this Swisyn sample is 6949648f8c2740ed5ea0ab9fe95b0326.
Strike Swisyn_7954f536	This strike sends a malware sample known as Swisyn. Swisyn is a loader that installs malicious software on the system, including remote access tool functionality, allowing the controller to perform any malicious action. The MD5 hash of this Swisyn sample is 7954f536503d9016dadaf9ae06f5a5ef.
Strike Swisyn_8e804a33	This strike sends a malware sample known as Swisyn. Swisyn is a loader that installs malicious software on the system, including remote access tool functionality, allowing the controller to perform any malicious action. The MD5 hash of this Swisyn sample is 8e804a339c9161bc85356fc84016b7b5.
Strike Swisyn_980749e4	This strike sends a malware sample known as Swisyn. Swisyn is a loader that installs malicious software on the system, including remote access tool functionality, allowing the controller to perform any malicious action. The MD5 hash of this Swisyn sample is 980749e4a0ed0362d66b12a26471e807.
Strike Swisyn_b19d3c9a	This strike sends a malware sample known as Swisyn. Swisyn is a loader that installs malicious software on the system, including remote access tool functionality, allowing the controller to perform any malicious action. The MD5 hash of this Swisyn sample is b19d3c9a48265ce37b1d246dd7ef76a7.
Strike Swisyn_d6a8e57a	This strike sends a malware sample known as Swisyn. Swisyn is a loader that installs malicious software on the system, including remote access tool functionality, allowing the controller to perform any malicious action. The MD5 hash of this Swisyn sample is d6a8e57addc7e4c4075435d7b5318364.
Strike Swisyn_edf4bc30	This strike sends a malware sample known as Swisyn. Swisyn is a loader that installs malicious software on the system, including remote access tool functionality, allowing the controller to perform any malicious action. The MD5 hash of this Swisyn sample is edf4bc30b9c905890317079156c84fbb.

<b>Name</b>	<b>Description</b>
Strike SysJoker_2eaf0c5	<p>This strike sends a malware sample known as SysJoker. SysJoker RAT is a cross-platform malware which targets Windows, Linux and macOS operating systems. This variant of the malware is written in Rust and since it is cross-platform it allows the malware authors to gain advantage of wide infection on all major platforms. SysJoker can execute commands remotely as well as download and execute new malware on victim machines. SysJoker contacts a URL on OneDrive to retrieve the C2 server address. Using OneDrive allows the attackers to easily change the C2 address, which enables them to stay ahead of different reputation-based services. The major functionality remains the same in all three platforms due to its shared code. The MD5 hash of this SysJoker sample is 2eaf0c5c2bf567631e08c999edb17cd.</p>
Strike SysJoker_31c2813c	<p>This strike sends a malware sample known as SysJoker. SysJoker RAT is a cross-platform malware which targets Windows, Linux and macOS operating systems. This variant of the malware is written in Rust and since it is cross-platform it allows the malware authors to gain advantage of wide infection on all major platforms. SysJoker can execute commands remotely as well as download and execute new malware on victim machines. SysJoker contacts a URL on OneDrive to retrieve the C2 server address. Using OneDrive allows the attackers to easily change the C2 address, which enables them to stay ahead of different reputation-based services. The major functionality remains the same in all three platforms due to its shared code. The MD5 hash of this SysJoker sample is 31c2813c1fb1e42b85014b2fc3fe0666.</p>
Strike SysJoker_9416d7dc	<p>This strike sends a malware sample known as SysJoker. SysJoker RAT is a cross-platform malware which targets Windows, Linux and macOS operating systems. This variant of the malware is written in Rust and since it is cross-platform it allows the malware authors to gain advantage of wide infection on all major platforms. SysJoker can execute commands remotely as well as download and execute new malware on victim machines. SysJoker contacts a URL on OneDrive to retrieve the C2 server address. Using OneDrive allows the attackers to easily change the C2 address, which enables them to stay ahead of different reputation-based services. The major functionality remains the same in all three platforms due to its shared code. The MD5 hash of this SysJoker sample is 9416d7dc2ecdeda92ba35cd5e54eb044.</p>
Strike SysJoker_c2848b4e	<p>This strike sends a malware sample known as SysJoker. SysJoker RAT is a cross-platform malware which targets Windows, Linux and macOS operating systems. This variant of the malware is written in Rust and since it is cross-platform it allows the malware authors to gain advantage of wide infection on all major platforms. SysJoker can execute commands remotely as well as download and execute new malware on victim machines. SysJoker contacts a URL on OneDrive to retrieve the C2 server address. Using OneDrive allows the attackers to easily change the C2 address, which enables them to stay ahead of different reputation-based services. The major functionality remains the same in all three platforms due to its shared code. The MD5 hash of this SysJoker sample is c2848b4e34b45e095bd8e764ca1a4fdd.</p>

<b>Name</b>	<b>Description</b>
Strike SysJoker_d51e617f	This strike sends a malware sample known as SysJoker. SysJoker RAT is a cross-platform malware which targets Windows, Linux and macOS operating systems. This variant of the malware is written in Rust and since it is cross-platform it allows the malware authors to gain advantage of wide infection on all major platforms. SysJoker can execute commands remotely as well as download and execute new malware on victim machines. SysJoker contacts a URL on OneDrive to retrieve the C2 server address. Using OneDrive allows the attackers to easily change the C2 address, which enables them to stay ahead of different reputation-based services. The major functionality remains the same in all three platforms due to its shared code. The MD5 hash of this SysJoker sample is d51e617fe1c1962801ad5332163717bb.
Strike TA402_0de40d66	This strike sends a malware sample known as TA402. This sample belongs to TA402 malware campaign that targets Middle Eastern and North African Government Entities, employing the IronWind downloader. They utilize weaponized XLL and RAR files to evade detection. The campaign involves phishing emails that pose as economic affairs messages. These emails lead to the download of a malicious Microsoft PowerPoint Add-in (PPAM) file containing IronWind and additional components. The malware utilizes a C2 domain and executes a multi-stage infection process that involves shellcode and .NET loaders. The MD5 hash of this TA402 sample is 0de40d666d23ecfd3d6b12f0ce567631.
Strike TA402_0e24fa3b	This strike sends a malware sample known as TA402. This sample belongs to TA402 malware campaign that targets Middle Eastern and North African Government Entities, employing the IronWind downloader. They utilize weaponized XLL and RAR files to evade detection. The campaign involves phishing emails that pose as economic affairs messages. These emails lead to the download of a malicious Microsoft PowerPoint Add-in (PPAM) file containing IronWind and additional components. The malware utilizes a C2 domain and executes a multi-stage infection process that involves shellcode and .NET loaders. The MD5 hash of this TA402 sample is 0e24fa3bb4de4977e68fa4438c025d9d.
Strike TA402_66572a74	This strike sends a malware sample known as TA402. This sample belongs to TA402 malware campaign that targets Middle Eastern and North African Government Entities, employing the IronWind downloader. They utilize weaponized XLL and RAR files to evade detection. The campaign involves phishing emails that pose as economic affairs messages. These emails lead to the download of a malicious Microsoft PowerPoint Add-in (PPAM) file containing IronWind and additional components. The malware utilizes a C2 domain and executes a multi-stage infection process that involves shellcode and .NET loaders. The MD5 hash of this TA402 sample is 66572a740d26abf3ea131704957ff7a6.
Strike TA402_70f3b724	This strike sends a malware sample known as TA402. This sample belongs to TA402 malware campaign that targets Middle Eastern and North African Government Entities, employing the IronWind downloader. They utilize weaponized XLL and RAR files to evade detection. The campaign involves phishing emails that pose as economic affairs messages. These emails lead to the download of a malicious Microsoft PowerPoint Add-in (PPAM) file containing IronWind and additional components. The malware utilizes a C2 domain and executes a multi-stage infection process that involves shellcode and .NET loaders. The MD5 hash of this TA402 sample is 70f3b7246019262bf981d9266c7aadb4.

<b>Name</b>	<b>Description</b>
Strike TA402_88915eb5	This strike sends a malware sample known as TA402. This sample belongs to TA402 malware campaign that targets Middle Eastern and North African Government Entities, employing the IronWind downloader. They utilize weaponized XLL and RAR files to evade detection. The campaign involves phishing emails that pose as economic affairs messages. These emails lead to the download of a malicious Microsoft PowerPoint Add-in (PPAM) file containing IronWind and additional components. The malware utilizes a C2 domain and executes a multi-stage infection process that involves shellcode and .NET loaders. The MD5 hash of this TA402 sample is 88915eb58dc887d639845f3812338534.
Strike TA402_89f7d220	This strike sends a malware sample known as TA402. This sample belongs to TA402 malware campaign that targets Middle Eastern and North African Government Entities, employing the IronWind downloader. They utilize weaponized XLL and RAR files to evade detection. The campaign involves phishing emails that pose as economic affairs messages. These emails lead to the download of a malicious Microsoft PowerPoint Add-in (PPAM) file containing IronWind and additional components. The malware utilizes a C2 domain and executes a multi-stage infection process that involves shellcode and .NET loaders. The MD5 hash of this TA402 sample is 89f7d22009ba38b71aaa23db348e2ee1.
Strike TA402_943145d0	This strike sends a malware sample known as TA402. This sample belongs to TA402 malware campaign that targets Middle Eastern and North African Government Entities, employing the IronWind downloader. They utilize weaponized XLL and RAR files to evade detection. The campaign involves phishing emails that pose as economic affairs messages. These emails lead to the download of a malicious Microsoft PowerPoint Add-in (PPAM) file containing IronWind and additional components. The malware utilizes a C2 domain and executes a multi-stage infection process that involves shellcode and .NET loaders. The MD5 hash of this TA402 sample is 943145d0960ce1ff4fb586dee03c8471.
Strike TA402_ab0867d5	This strike sends a malware sample known as TA402. This sample belongs to TA402 malware campaign that targets Middle Eastern and North African Government Entities, employing the IronWind downloader. They utilize weaponized XLL and RAR files to evade detection. The campaign involves phishing emails that pose as economic affairs messages. These emails lead to the download of a malicious Microsoft PowerPoint Add-in (PPAM) file containing IronWind and additional components. The malware utilizes a C2 domain and executes a multi-stage infection process that involves shellcode and .NET loaders. The MD5 hash of this TA402 sample is ab0867d5376a12f00ca5fd06d628f8f4.
Strike TA402_e6b48973	This strike sends a malware sample known as TA402. This sample belongs to TA402 malware campaign that targets Middle Eastern and North African Government Entities, employing the IronWind downloader. They utilize weaponized XLL and RAR files to evade detection. The campaign involves phishing emails that pose as economic affairs messages. These emails lead to the download of a malicious Microsoft PowerPoint Add-in (PPAM) file containing IronWind and additional components. The malware utilizes a C2 domain and executes a multi-stage infection process that involves shellcode and .NET loaders. The MD5 hash of this TA402 sample is e6b489737b3a22fbc8bf85de00081a5c.

<b>Name</b>	<b>Description</b>
Strike TA402_f321fcbf	This strike sends a malware sample known as TA402. This sample belongs to TA402 malware campaign that targets Middle Eastern and North African Government Entities, employing the IronWind downloader. They utilize weaponized XLL and RAR files to evade detection. The campaign involves phishing emails that pose as economic affairs messages. These emails lead to the download of a malicious Microsoft PowerPoint Add-in (PPAM) file containing IronWind and additional components. The malware utilizes a C2 domain and executes a multi-stage infection process that involves shellcode and .NET loaders. The MD5 hash of this TA402 sample is f321fcbfa16d92fde8c4bad1b0968140.
Strike Tedy_00c66c0c	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 00c66c0c82d5c8320949e460113b4dad.
Strike Tedy_05a256fe	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 05a256fed9a630fd019f8058cacd6671.
Strike Tedy_1eaf7811	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 1eaf7811e69828815b4f507ed2e0202e.
Strike Tedy_264c080f	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 264c080f99eaef56529cfcbf70253b2b.
Strike Tedy_33d2ff5e	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 33d2ff5e884ddedf8e1317c439ed39c0.
Strike Tedy_3b417b51	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 3b417b51e1d7c4289a47fb07cfaf309fd.
Strike Tedy_4b0fc06e	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 4b0fc06e26def68687a31f8c73cd6832.
Strike Tedy_4be22ca0	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 4be22ca0bab2e1a0f4c021886f2ab8cf.

<b>Name</b>	<b>Description</b>
Strike Tedy_56feb85d	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 56feb85d714c7948276a75e602456870.
Strike Tedy_761f7e63	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 761f7e6376a6a9c40d23b3200f4ca1f8.
Strike Tedy_7abbdaa5	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 7abbdaa5255631386ebae72be3116241.
Strike Tedy_7e054d33	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 7e054d3383a3c9c12872fa981270c6b8.
Strike Tedy_81141b39	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 81141b395d0b88a14e99f8000cbad627.
Strike Tedy_8f3acb97	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 8f3acb97f557779e8077c770fd4dbf24.
Strike Tedy_91a577d1	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 91a577d1062878b7c876df4e50aa32e6.
Strike Tedy_9ecdc144	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is 9ecdc14407aa3de63172279327098314.
Strike Tedy_a4231b7b	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is a4231b7b84af3176630d8c43c42c841b.
Strike Tedy_ac3fe0ef	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is ac3fe0efb8de93015be67721acafc50a.

<b>Name</b>	<b>Description</b>
Strike Tedy_ccdf896f	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is ccdf896feed2fd8914380666c415edc2.
Strike Tedy_dcead5a2	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is dcead5a20776ab7d56c7be346905a6b9.
Strike Tedy_dfe16a95	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is dfe16a95cca72acb7ef3557af0fb5703.
Strike Tedy_e7b47211	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is e7b4721184f98f7e6548938f4495eaab.
Strike Tedy_f07edfc0d	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is f07edfc0d02e0bd17ccfc5c24cbe41466.
Strike Tedy_f9f1fd79	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is f9f1fd79bb53bf281c89cc03e3ce315f.
Strike Tedy_fdba3070	This strike sends a malware sample known as Tedy. Tedy malware will modify the system registry keys. This malware may also download additional malware. This sample may have been compressed with a packer. The MD5 hash of this Tedy sample is fdba30700880887d2c8234c93121e460.
Strike TerraLogger_08fef6e1	This strike sends a malware sample known as TerraLogger. TerraLogger is a malware family linked to the Golden Chickens aka Venom Spider threat group. The group is known as a MaaS platform used in cybercriminal activity. TerraLogger is a keylogger that uses keyboard hooks to record keystrokes. The MD5 hash of this TerraLogger sample is 08fef6e11058478fd1c5bb46d5d937a3.
Strike TerraLogger_10155c41	This strike sends a malware sample known as TerraLogger. TerraLogger is a malware family linked to the Golden Chickens aka Venom Spider threat group. The group is known as a MaaS platform used in cybercriminal activity. TerraLogger is a keylogger that uses keyboard hooks to record keystrokes. The MD5 hash of this TerraLogger sample is 10155c41825d728b745d783d3b0e901a.
Strike TerraLogger_d7f3c2b1	This strike sends a malware sample known as TerraLogger. TerraLogger is a malware family linked to the Golden Chickens aka Venom Spider threat group. The group is known as a MaaS platform used in cybercriminal activity. TerraLogger is a keylogger that uses keyboard hooks to record keystrokes. The MD5 hash of this TerraLogger sample is d7f3c2b15e4a90a56eaf5a17c90b3caa.

<b>Name</b>	<b>Description</b>
Strike TerraLogger_f94a5977	This strike sends a malware sample known as TerraLogger. TerraLogger is a malware family linked to the Golden Chickens aka Venom Spider threat group. The group is known as a MaaS platform used in cybercriminal activity. TerraLogger is a keylogger that uses keyboard hooks to record keystrokes. The MD5 hash of this TerraLogger sample is f94a5977434add69333b9670f224684a.
Strike TerraStealerV2_51dab940	This strike sends a malware sample known as TerraStealerV2. TerraStealerV2 is a malware family linked to the Golden Chickens aka Venom Spider threat group. The group is known as a MaaS platform used in cybercriminal activity. TerraStealerV2 collects browser credentials and other victim information like cryptocurrency wallet data, and extension information. It uses Telegram to exfiltrate this data back to the attacker. The MD5 hash of this TerraStealerV2 sample is 51dab940b8a53f27586a707eda07e2e9.
Strike TerraStealerV2_675f1b64	This strike sends a malware sample known as TerraStealerV2. TerraStealerV2 is a malware family linked to the Golden Chickens aka Venom Spider threat group. The group is known as a MaaS platform used in cybercriminal activity. TerraStealerV2 collects browser credentials and other victim information like cryptocurrency wallet data, and extension information. It uses Telegram to exfiltrate this data back to the attacker. The MD5 hash of this TerraStealerV2 sample is 675f1b648b3e8810a4a32fe32546490b.
Strike TerraStealerV2_93b99539	This strike sends a malware sample known as TerraStealerV2. TerraStealerV2 is a malware family linked to the Golden Chickens aka Venom Spider threat group. The group is known as a MaaS platform used in cybercriminal activity. TerraStealerV2 collects browser credentials and other victim information like cryptocurrency wallet data, and extension information. It uses Telegram to exfiltrate this data back to the attacker. The MD5 hash of this TerraStealerV2 sample is 93b99539a720ff7bc27eaef677d29c9a.
Strike TeslaCrypt_00658cac	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this TeslaCrypt sample is 00658caca94f6d736a67b553302c7980.
Strike TeslaCrypt_01df1af3	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 01df1af3f09abbea8a92331c7305356b.
Strike TeslaCrypt_02689622	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 02689622ffb34c0b816a26f937bc2c8.
Strike TeslaCrypt_0885115c	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 0885115c42ce73bb06cbe4b1a55e7c91.
Strike TeslaCrypt_0d730d28	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 0d730d28609da65b0ac3ac3f66a085ef.

<b>Name</b>	<b>Description</b>
Strike TeslaCrypt_0d8ff116	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 0d8ff116ce8976fc820c996a6ee90c3a.
Strike TeslaCrypt_107d78d4	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 107d78d430162b5c3fcfd6f5a99c74fb.
Strike TeslaCrypt_12e2de7b	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 12e2de7b31f247cf6eb48c7164b2c8df.
Strike TeslaCrypt_13fd1e01	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this TeslaCrypt sample is 13fd1e01e5f24b6a7aeeef996235ca886.
Strike TeslaCrypt_170e75ff	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has a new section added in the PE file format with random contents. The MD5 hash of this TeslaCrypt sample is 170e75ffff7010ecec4d6b282149d0ba.
Strike TeslaCrypt_1a0731a3	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 1a0731a3fde61b4f8d190fe11a6022ab.
Strike TeslaCrypt_1a1f3710	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 1a1f3710088a7a5c062ad9c43b0628f8.
Strike TeslaCrypt_20238f80	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 20238f801e16af46fc3eaf64cb6e6126.
Strike TeslaCrypt_25a8164a	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 25a8164a44d68e0989967bec65e2818d.
Strike TeslaCrypt_2850b227	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has a new section added in the PE file format with random contents. The MD5 hash of this TeslaCrypt sample is 2850b22756a0e1cf164d0801bc0430ff.
Strike TeslaCrypt_29d80860	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has random bytes appended at the end of the file. The MD5 hash of this TeslaCrypt sample is 29d80860c96bacff05812456d7621754.

<b>Name</b>	<b>Description</b>
Strike TeslaCrypt_2d4d0fa0	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 2d4d0fa03435636ea85e603be1055031.
Strike TeslaCrypt_36b9c9f9	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 36b9c9f9f3e9b07ec4f9d5c273e3b9de.
Strike TeslaCrypt_38602df4	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 38602df4390dbda254d40126d7d992b2.
Strike TeslaCrypt_3cb16522	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has the checksum removed in the PE file format. The MD5 hash of this TeslaCrypt sample is 3cb16522d05fbded5f94226d7d4f6ed8.
Strike TeslaCrypt_3d1d2104	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 3d1d21040e9d68cbf02e146ad0ad67eb.
Strike TeslaCrypt_412f4761	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 412f4761dcf9e20ad8a05a16663fbc7e.
Strike TeslaCrypt_4345e8d9	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this TeslaCrypt sample is 4345e8d98cb826d3f493ad03ebdf2f46.
Strike TeslaCrypt_4573ead0	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has the timestamp field updated in the PE file header. The MD5 hash of this TeslaCrypt sample is 4573ead04797a7287b4c320e46042cc3.
Strike TeslaCrypt_48e0d4d3	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 48e0d4d3fba9365813688afdf9bfbd1f.
Strike TeslaCrypt_4ae42e33	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 4ae42e33f8104a47ae1b19542607f753.
Strike TeslaCrypt_4bc07d04	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 4bc07d04b3a595d727461619e72b8af2.

<b>Name</b>	<b>Description</b>
Strike TeslaCrypt_4bdd826e	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 4bdd826e9cd92d7cd6a44d36d8793301.
Strike TeslaCrypt_4d69c441	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 4d69c441231bad3e39da8230388920e5.
Strike TeslaCrypt_509f3621	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 509f3621ccd1590cbc7b7f87de9649f2.
Strike TeslaCrypt_5104dda9	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 5104dda9b6b6558fcfd70c784f56cacd.
Strike TeslaCrypt_54dff53b	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 54dff53b7630c027c95c7285dd8d001e.
Strike TeslaCrypt_557e0286	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 557e0286e6a1ddf962180d0aef426f56.
Strike TeslaCrypt_55b87f03	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has been packed using upx packer, with the default options. The MD5 hash of this TeslaCrypt sample is 55b87f0397e4600386250f2047c773c4.
Strike TeslaCrypt_57b0420e	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 57b0420ebd965ccc489ab60cde9320a0.
Strike TeslaCrypt_584e49db	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 584e49dbe037b315b67b79a7f9a404eb.
Strike TeslaCrypt_5869bba8	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 5869bba88bcd0a572bdf48bf79a96084.
Strike TeslaCrypt_5c6911fb	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this TeslaCrypt sample is 5c6911fb1f0dca9df6cabd7c83d9814f.
Strike TeslaCrypt_6127d0d5	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 6127d0d566524543ede893d4713d4ea5.

<b>Name</b>	<b>Description</b>
Strike TeslaCrypt_6215feec	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 6215feecc1e772a83859ced35318ed2b.
Strike TeslaCrypt_6266203e	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 6266203ec37b67ad31e71d3216f3fe90.
Strike TeslaCrypt_63d2e5b7	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has a new section added in the PE file format with random contents. The MD5 hash of this TeslaCrypt sample is 63d2e5b72bcd3fd3b0f3b29ada81841a.
Strike TeslaCrypt_6626b29f	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 6626b29fab9e9465d265344871bc897e.
Strike TeslaCrypt_69d66bd8	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 69d66bd8dc40d804d2896855b381d1c7.
Strike TeslaCrypt_6af11c2d	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 6af11c2d6e86170a456fcabe79d7cdfe.
Strike TeslaCrypt_751ec5f3	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 751ec5f39b6fe277cad8374f11331f15.
Strike TeslaCrypt_76f35d2e	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has random bytes appended at the end of the file. The MD5 hash of this TeslaCrypt sample is 76f35d2e565f0d04ccafb16742520272.
Strike TeslaCrypt_796aa3c8	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 796aa3c80d4b3be5333cbc910071612a.
Strike TeslaCrypt_7b079fdf	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 7b079fdfae4d32274dc53ba03fc7cb51.
Strike TeslaCrypt_818fe0f4	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has been packed using upx packer, with the default options. The MD5 hash of this TeslaCrypt sample is 818fe0f40198d785ce706bd80319cfe1.

<b>Name</b>	<b>Description</b>
Strike TeslaCrypt_8489707b	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 8489707b1115144a60e83e85d79eb0d0.
Strike TeslaCrypt_854bca4d	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 854bca4dcd3f09e07df658db8c2daed0.
Strike TeslaCrypt_8915b658	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 8915b658510bbaa95c236ae4a82cced4.
Strike TeslaCrypt_8a5d6838	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 8a5d68384093d008fded0bbcfcf29fc42.
Strike TeslaCrypt_944c417c	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this TeslaCrypt sample is 944c417c908647ea786aa836dcf87289.
Strike TeslaCrypt_975117b1	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 975117b1c5fd0363e160b381280a33fe.
Strike TeslaCrypt_991ff593	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is 991ff593a3b9b297ef6e2563b47f2d82.
Strike TeslaCrypt_9b77979f	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this TeslaCrypt sample is 9b77979fed5ef112cc96f9554f903842.
Strike TeslaCrypt_9d13bae9	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has the timestamp field updated in the PE file header. The MD5 hash of this TeslaCrypt sample is 9d13bae96cf4e77b52e630586907ac16.
Strike TeslaCrypt_a0ad76a6	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is a0ad76a66a5e8cf5daea3158acff1c29.
Strike TeslaCrypt_a1606deb	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is a1606deb54f2d523cf7d2266179fdf70.

<b>Name</b>	<b>Description</b>
Strike TeslaCrypt_a48b4000	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is a48b4000ec1866cb6e7a23b5bdbe37db.
Strike TeslaCrypt_a874ef39	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is a874ef3926e59eac0b158fd5e6a9a35f.
Strike TeslaCrypt_af3c3d0d	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is af3c3d0d579ee843d7957d1a1423f2fc.
Strike TeslaCrypt_b345e64a	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is b345e64a78fb601f096abf9e024ca89c.
Strike TeslaCrypt_b3b0743d	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is b3b0743dc39bf9963736e85f61002134.
Strike TeslaCrypt_b6d8812f	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is b6d8812fc7198cf125d15e280e7ce8fc.
Strike TeslaCrypt_c0fb9afc	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has the checksum removed in the PE file format. The MD5 hash of this TeslaCrypt sample is c0fb9afc7f80a40fc173f6ff0c42d227.
Strike TeslaCrypt_c24ddf1c	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is c24ddf1ca6c1f26653f29e0e24a83f2c.
Strike TeslaCrypt_c318cb9a	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is c318cb9a36f9c7ee5b15b589ed7b594f.
Strike TeslaCrypt_c32375be	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is c32375be2b606807f997c0d68dcc0b8a.
Strike TeslaCrypt_c4644580	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary file has one more imports added in the import table. The MD5 hash of this TeslaCrypt sample is c464458070c7909d7de471e5630592f0.
Strike TeslaCrypt_cb7d4940	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is cb7d494023414e8d71f14a39b9819e3c.

<b>Name</b>	<b>Description</b>
Strike TeslaCrypt_cea7506c	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is cea7506c22e161b3703543ee421f70c8.
Strike TeslaCrypt_cf4612e2	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this TeslaCrypt sample is cf4612e28ccf1a1476429f463116d6cc.
Strike TeslaCrypt_d05d1a0c	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is d05d1a0c12ab22e18f491d6e14c22eb5.
Strike TeslaCrypt_d9807993	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is d9807993573f3877545868116b424bc7.
Strike TeslaCrypt_da37801e	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is da37801eb453924749147d77069cb557.
Strike TeslaCrypt_db8af569	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is db8af56918c0c3fa87d1c1a631ab423c.
Strike TeslaCrypt_dd587d20	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is dd587d20de9a14d86bdbc4ed94584038.
Strike TeslaCrypt_e126aa94	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is e126aa94d0d2ac98f9baa482bf48672a.
Strike TeslaCrypt_e12714cc	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is e12714cc500326d836bc2e13b195977a.
Strike TeslaCrypt_e747b47b	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is e747b47bf6413c1c9c8b390c1d6968f3.
Strike TeslaCrypt_e99bd4d8	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is e99bd4d8d715d93645c3850fc2c2e1d3.
Strike TeslaCrypt_eae946a1	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is eae946a10a840370d1d8ddb919b284f2.

<b>Name</b>	<b>Description</b>
Strike TeslaCrypt_f00ffef3	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has the checksum removed in the PE file format. The MD5 hash of this TeslaCrypt sample is f00ffef31cf1df10a9d06e6b931798b7.
Strike TeslaCrypt_f15f513d	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is f15f513d2a3784e9b56bd2f80dc6f088.
Strike TeslaCrypt_f27112dc	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is f27112dc5d2e62d0f6748b1478bd3578.
Strike TeslaCrypt_f5c24ce9	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is f5c24ce99fc9ffc9ff25cf8bdfe7c033.
Strike TeslaCrypt_f61b3c14	This strike sends a polymorphic malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this TeslaCrypt sample is f61b3c14d032796e892fda0214bb6ada.
Strike TeslaCrypt_f7edddc4	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is f7edddc47a40465556c2b75cccd972e1d.
Strike TeslaCrypt_f8c510f5	This strike sends a malware sample known as TeslaCrypt. This ransomware demands Bitcoin in order to decrypt files from the system. The MD5 hash of this TeslaCrypt sample is f8c510f569bb2daf365c01e002e9bf48.
Strike Thanos_03b76a51	This strike sends a malware sample known as Thanos. Thanos ransomware offers the user the option to customize and include a variety of functions and capabilities. The Thanos builder code was recently made available and many variants have started to surface with its framework at the core. This version of Thanos includes the ability to overwrite the MBR and display the same ransom message, as well as the ability to detect and evade analysis tools. The MD5 hash of this Thanos sample is 03b76a5130d0df8134a6bdea7fe97bcd.
Strike Thanos_18cec1f1	This strike sends a polymorphic malware sample known as Thanos. Thanos ransomware offers the user the option to customize and include a variety of functions and capabilities. The Thanos builder code was recently made available and many variants have started to surface with its framework at the core. This version of Thanos includes the ability to overwrite the MBR and display the same ransom message, as well as the ability to detect and evade analysis tools. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Thanos sample is 18cec1f15061129aff9fa49bc639dbbe.

<b>Name</b>	<b>Description</b>
Strike Thanos_1d45efc7	This strike sends a polymorphic malware sample known as Thanos. Thanos ransomware offers the user the option to customize and include a variety of functions and capabilities. The Thanos builder code was recently made available and many variants have started to surface with its framework at the core. This version of Thanos includes the ability to overwrite the MBR and display the same ransom message, as well as the ability to detect and evade analysis tools. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Thanos sample is 1d45efc7078b10c28a1d606053d066af.
Strike Thanos_be60e389	This strike sends a malware sample known as Thanos. Thanos ransomware offers the user the option to customize and include a variety of functions and capabilities. The Thanos builder code was recently made available and many variants have started to surface with its framework at the core. This version of Thanos includes the ability to overwrite the MBR and display the same ransom message, as well as the ability to detect and evade analysis tools. The MD5 hash of this Thanos sample is be60e389a0108b2871dff12dfbb542ac.
Strike Thanos_d6d95626	This strike sends a malware sample known as Thanos. Thanos ransomware offers the user the option to customize and include a variety of functions and capabilities. The Thanos builder code was recently made available and many variants have started to surface with its framework at the core. This version of Thanos includes the ability to overwrite the MBR and display the same ransom message, as well as the ability to detect and evade analysis tools. The MD5 hash of this Thanos sample is d6d956267a268c9dcf48445629d2803e.
Strike Thanos_e01e11dc	This strike sends a malware sample known as Thanos. Thanos ransomware offers the user the option to customize and include a variety of functions and capabilities. The Thanos builder code was recently made available and many variants have started to surface with its framework at the core. This version of Thanos includes the ability to overwrite the MBR and display the same ransom message, as well as the ability to detect and evade analysis tools. The MD5 hash of this Thanos sample is e01e11dca5e8b08fc8231b1cb6e2048c.
Strike TinyBanker_10b587c2	This strike sends a malware sample known as TinyBanker. The malware TinyBanker, also known as Zusy or Tinba, is a trojan that uses a javascript injected form to steal banking information. When executed, it injects itself into Windows processes like "explorer.exe" and "winver.exe. The MD5 hash of this TinyBanker sample is 10b587c21e9e11de2c9815423f035095.
Strike TinyBanker_2fc76498	This strike sends a malware sample known as TinyBanker. The malware TinyBanker, also known as Zusy or Tinba, is a trojan that uses a javascript injected form to steal banking information. When executed, it injects itself into Windows processes like "explorer.exe" and "winver.exe. The MD5 hash of this TinyBanker sample is 2fc764982d67accb3b0f94fb7e19ef94.
Strike TinyBanker_b20386f9	This strike sends a malware sample known as TinyBanker. The malware TinyBanker, also known as Zusy or Tinba, is a trojan that uses a javascript injected form to steal banking information. When executed, it injects itself into Windows processes like "explorer.exe" and "winver.exe. The MD5 hash of this TinyBanker sample is b20386f967f4214050b3c18f5d335f9c.

<b>Name</b>	<b>Description</b>
Strike TinyBanker_ebf2fb86	This strike sends a malware sample known as TinyBanker. The malware TinyBanker, also known as Zusy or Tinba, is a trojan that uses a javascript injected form to steal banking information. When executed, it injects itself into Windows processes like "explorer.exe" and "winver.exe. The MD5 hash of this TinyBanker sample is ebf2fb861086af8914d60d11d6451977.
Strike ToddyCat_0f7002aa	This strike sends a malware sample known as ToddyCat. This sample is a ToddyCat Loader. ToddyCat is an APT actor that was previously detected attacking high profile target's Microsoft Exchange Servers. Their attacks utilize numerous malware loaders which are invoked by several executables including rundll32.exe, and VLC.exe. ToddyCat's latest attacks use these loaders as well as other trojans to collect and exfiltrate sensitive information from the target. The MD5 hash of this ToddyCat sample is 0f7002aaca8c1e71959c3ee635a85f14.
Strike ToddyCat_90b14807	This strike sends a malware sample known as ToddyCat. This sample is a ToddyCat Loader. ToddyCat is an APT actor that was previously detected attacking high profile target's Microsoft Exchange Servers. Their attacks utilize numerous malware loaders which are invoked by several executables including rundll32.exe, and VLC.exe. ToddyCat's latest attacks use these loaders as well as other trojans to collect and exfiltrate sensitive information from the target. The MD5 hash of this ToddyCat sample is 90b14807734045f1e0a47c40df949ac4.
Strike ToddyCat_97d0a47b	This strike sends a malware sample known as ToddyCat. This sample is a ToddyCat Loader. ToddyCat is an APT actor that was previously detected attacking high profile target's Microsoft Exchange Servers. Their attacks utilize numerous malware loaders which are invoked by several executables including rundll32.exe, and VLC.exe. ToddyCat's latest attacks use these loaders as well as other trojans to collect and exfiltrate sensitive information from the target. The MD5 hash of this ToddyCat sample is 97d0a47b595a20a3944919863a8163d1.
Strike ToddyCat_bebbeba3	This strike sends a malware sample known as ToddyCat. This sample is a ToddyCat Loader. ToddyCat is an APT actor that was previously detected attacking high profile target's Microsoft Exchange Servers. Their attacks utilize numerous malware loaders which are invoked by several executables including rundll32.exe, and VLC.exe. ToddyCat's latest attacks use these loaders as well as other trojans to collect and exfiltrate sensitive information from the target. The MD5 hash of this ToddyCat sample is bebbeba37667453003d2372103c45bbf.
Strike ToddyCat_d3050b3c	This strike sends a malware sample known as ToddyCat. This sample is a ToddyCat Loader. ToddyCat is an APT actor that was previously detected attacking high profile target's Microsoft Exchange Servers. Their attacks utilize numerous malware loaders which are invoked by several executables including rundll32.exe, and VLC.exe. ToddyCat's latest attacks use these loaders as well as other trojans to collect and exfiltrate sensitive information from the target. The MD5 hash of this ToddyCat sample is d3050b3c7ee8a80d8d67006246266d.

<b>Name</b>	<b>Description</b>
Strike ToddyCat_d4d8131e	This strike sends a malware sample known as ToddyCat. This sample is a ToddyCat Loader. ToddyCat is an APT actor that was previously detected attacking high profile target's Microsoft Exchange Servers. Their attacks utilize numerous malware loaders which are invoked by several executables including rundll32.exe, and VLC.exe. ToddyCat's latest attacks use these loaders as well as other trojans to collect and exfiltrate sensitive information from the target. The MD5 hash of this ToddyCat sample is d4d8131ed03b71d58b1ba348f9606df7.
Strike Tofsee_03d12b8e	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is 03d12b8e29cbd18b673cedb0f7f86d5c.
Strike Tofsee_12125ce0	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is 12125ce015e5fba34c2c3bac921a9f86.
Strike Tofsee_1256c61a	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is 1256c61ada24718d6b0cc42c36c0ab10.
Strike Tofsee_194cf82e	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is 194cf82e76ce8a5b05cbae71a892867a.
Strike Tofsee_468df98d	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is 468df98df8cb4d17f1bf59dabb5431ee.

<b>Name</b>	<b>Description</b>
Strike Tofsee_4880a2fe	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is 4880a2fecf841b3240a81e4dc09e6fae.
Strike Tofsee_5753474b	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is 5753474b849e19b4f01031db304a79c4.
Strike Tofsee_80ab43e7	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is 80ab43e77b53fe54bb824639ac3f0a1c.
Strike Tofsee_8a9166da	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is 8a9166dac7113acaf058280e65ff78d0.
Strike Tofsee_9aa860e5	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is 9aa860e53a8e63e3307140ece140db80.
Strike Tofsee_b130c37e	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is b130c37e492949683b222e530a435769.

<b>Name</b>	<b>Description</b>
Strike Tofsee_b6fba6a2	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is b6fba6a2d04ffaa0834c71357d563ed8.
Strike Tofsee_c1b67151	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is c1b6715166fbda0eb2f28189b6e1cb43.
Strike Tofsee_c618b909	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is c618b909f00266bbd07c0e7429e6d228.
Strike Tofsee_ca0d7ab4	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is ca0d7ab4ec6def337cc1bc781ce091f0.
Strike Tofsee_dc4b262a	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is dc4b262a11999bdd8882a791ffd7bdca.
Strike Tofsee_e472ee3e	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is e472ee3e314ec90bffe73a273eab982.

<b>Name</b>	<b>Description</b>
Strike Tofsee_e9f4b1d3	This strike sends a malware sample known as Tofsee. Tofsee is multi-purpose malware that features a number of modules used to carry out various activities, such as sending spam messages, conducting click fraud, mining cryptocurrency and more. Infected systems become part of the Tofsee spam botnet and are used to send large volumes of spam messages in an effort to infect additional systems and increase the overall size of the botnet under the operator's control. The MD5 hash of this Tofsee sample is e9f4b1d3297a640bb0fb221cb0da1441.
Strike TookPS_8d1e20b5	This strike sends a malware sample known as TookPS. TookPS is a malware downloader. Once infected it begins outbound communication with the attacker C2 server. From here it retrieves commands that allow additional malware to be downloaded to establish a backdoor and allow for remote access. The MD5 hash of this TookPS sample is 8d1e20b5f2d89f62b4fb7f90bc8e29f6.
Strike TrickBot_010c5005	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 010c50055f097fa6bb7d839d3147a2ea.
Strike TrickBot_014be42c	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 014be42cda8eb56cfea80892e736e7c1.
Strike TrickBot_01df6398	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 01df63985a519b2d6447998cceada56b.
Strike TrickBot_04420a52	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 04420a52469fa8c3dece0126fdeb7e80.
Strike TrickBot_0455b17e	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this TrickBot sample is 0455b17ef0b235a3c4dcc9a66e5305e2.
Strike TrickBot_07c5e05b	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 07c5e05b52e1bcc7492266b46982f9e5.

<b>Name</b>	<b>Description</b>
Strike TrickBot_09573d0a	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 09573d0a0c60a957c9e80d06a11b442e.
Strike TrickBot_0a5281c9	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 0a5281c935c5791663b702895803719e.
Strike TrickBot_0b183d62	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 0b183d6240d02bb57638033917e11e48.
Strike TrickBot_0e6371f8	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 0e6371f8f41dea8a620c65b0ca4a16a5.
Strike TrickBot_0f28b837	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 0f28b837de3e1ad653052a6c459683a4.
Strike TrickBot_0fbb702a	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 0fbb702ad70f4ad393a2d97c99289a15.
Strike TrickBot_105d2282	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 105d2282425a318a3c9d667ac8e5c7f2.
Strike TrickBot_13ad725b	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 13ad725b20bab4e16e23d07b37ba97b.

<b>Name</b>	<b>Description</b>
Strike TrickBot_15755349	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this TrickBot sample is 15755349b8ab974d167749fcf763bc80.
Strike TrickBot_15bdc351	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 15bdc351812c393bdfb6c4de694754d0.
Strike TrickBot_16ceee4b	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 16ceee4be1b477e97fd9046b40d7d65b.
Strike TrickBot_186d3ddb	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 186d3ddb5df74784da23a841ad7ae2da.
Strike TrickBot_1ac360fe	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 1ac360fef066d3c4b4db006c55371d43.
Strike TrickBot_1b4476b8	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this TrickBot sample is 1b4476b84e3eea57dece04f6682402cf.
Strike TrickBot_1fc6a697	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 1fc6a6970218db54923a3418851d9244.
Strike TrickBot_25ba363d	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 25ba363d1849134fd7943aa631d266be.

<b>Name</b>	<b>Description</b>
Strike TrickBot_26b8e22f	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 26b8e22f42fd00707aa625ec383731d9.
Strike TrickBot_26b8e67b	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this TrickBot sample is 26b8e67bbce94745b87a541c867f9ee8.
Strike TrickBot_274eb07e	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has the checksum removed in the PE file format. The MD5 hash of this TrickBot sample is 274eb07e2600acd6a62a508675ab6e09.
Strike TrickBot_2a4e6863	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 2a4e68634737e0655ce279c6211eac59.
Strike TrickBot_30ab319c	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this TrickBot sample is 30ab319cd8d08fcf96e06e8fb414499c.
Strike TrickBot_31990c04	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 31990c046c8824f192b49b2f9738265e.
Strike TrickBot_31e45c28	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 31e45c2854f8b176b718b5393c4e848d.
Strike TrickBot_32dfe14f	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 32dfe14fe473b36a31751b333f82c9e1.

<b>Name</b>	<b>Description</b>
Strike TrickBot_32e3a9c1	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 32e3a9c1efe10cbab7c8f15fd57e54a6.
Strike TrickBot_3779e428	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 3779e428792e9bf3703dfcf438cecd2b.
Strike TrickBot_3be39381	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 3be39381a1994f0055c41666e86221c7.
Strike TrickBot_3fe2eef9	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 3fe2eef9d6030683ee6bca5d180c85a5.
Strike TrickBot_421993b2	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 421993b2fc82e644b71d638028410316.
Strike TrickBot_453434b7	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 453434b724aeda596439430b12982cdd.
Strike TrickBot_4c44ea21	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 4c44ea21b98a995fb9cb39f485a80fea.
Strike TrickBot_4ce52d89	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary file has one more imports added in the import table. The MD5 hash of this TrickBot sample is 4ce52d89efff02ddd3995af5d69b65f4.

<b>Name</b>	<b>Description</b>
Strike TrickBot_4d9829c8	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 4d9829c8ddc45429fa8f40a758e821bf.
Strike TrickBot_4f25a15b	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 4f25a15bb2f5815f5b7a240cd88813b2.
Strike TrickBot_541f0951	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 541f09510b21a4da53450c48ef0f32f4.
Strike TrickBot_583bb559	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 583bb559817a3e82e9dbc39df68b216a.
Strike TrickBot_5cc6f3d0	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 5cc6f3d095282971693e9a7c1ea3c1d3.
Strike TrickBot_5d3242c3	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 5d3242c30060c66a18c7760adf582841.
Strike TrickBot_5d9d5845	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this TrickBot sample is 5d9d5845db1526c160a1cc0791cf49c.
Strike TrickBot_60da2209	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 60da22098eef105bd2768d317d8b81bc.

<b>Name</b>	<b>Description</b>
Strike TrickBot_629a37a7	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 629a37a7a921ffd9c6a46f42936dd86a.
Strike TrickBot_66d07e5c	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 66d07e5c7d5acb931603325b7e064d47.
Strike TrickBot_6adb52f5	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 6adb52f5787df2e229c6f7efa79b2ab8.
Strike TrickBot_6b553df5	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 6b553df50e52d6a374ca16adb25d2a53.
Strike TrickBot_6bb2cfbd	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 6bb2cfbd10aa288558b3a5d413056ed9.
Strike TrickBot_6c16b771	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 6c16b7715556744d54996256b431668a.
Strike TrickBot_6d0ab756	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 6d0ab7565c6a4094c6ae372747095c09.
Strike TrickBot_6d6da629	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 6d6da6296555ff0bb1b022431a05f6a2.
Strike TrickBot_741a22e5	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 741a22e524f0c165272d7d5881027253.

<b>Name</b>	<b>Description</b>
Strike TrickBot_747e2dff	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 747e2dff11b08670fbdc1632cfb8d394.
Strike TrickBot_74f95a32	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 74f95a32db60decf17b89113ed9e15e7.
Strike TrickBot_76376460	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 763764609377b0f3dbfa81a3cf8d9eff.
Strike TrickBot_7734c98f	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 7734c98fc19d785fb9bb15f160d8edfa.
Strike TrickBot_7c3b350d	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 7c3b350d98f0826e01dcfdf95d123477.
Strike TrickBot_82130c33	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 82130c33ba1635a09ab4d109a3ec6d0a.
Strike TrickBot_84834e1f	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 84834e1fc670e9375f83839273c886df.
Strike TrickBot_86a61b17	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 86a61b172e65df7eb61a576aa284b18f.
Strike TrickBot_87f56ddd	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 87f56ddd321f7c16fc1702e4112e7313.

<b>Name</b>	<b>Description</b>
Strike TrickBot_880c2f22	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 880c2f2214478fe32bcae2ba00715d77.
Strike TrickBot_894c0150	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 894c0150be02cd78f839f56434f1912b.
Strike TrickBot_8a341bdf	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 8a341bdf26de60144d5c5aab12f6227.
Strike TrickBot_8c3a027d	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 8c3a027dcfb199989fea5ba940e56052.
Strike TrickBot_8cc0021e	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 8cc0021e091932f84851a0bf9c02860b.
Strike TrickBot_8ce80634	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The Parent binary was packed using upx, hence this binary is the unpacked version generated using upx -d. The MD5 hash of this TrickBot sample is 8ce80634966cd3e73d24cc48b83cfe0e.
Strike TrickBot_938195ae	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 938195ae6a5ea077a43dccac2df43e0d.
Strike TrickBot_93d1113f	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 93d1113fa5b123b5cc537f1c74c81412.

<b>Name</b>	<b>Description</b>
Strike TrickBot_949e4fdd	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 949e4fddcd7de77db26dcraf532bf79a.
Strike TrickBot_97069b4b	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 97069b4b1647235a07d6630b18b8ab31.
Strike TrickBot_976b666c	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 976b666c2834842fa07d6ffaddafe98c.
Strike TrickBot_97a03d12	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 97a03d12f5c8dea0ae822a4a930871e9.
Strike TrickBot_988a76f0	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is 988a76f02c98bf4730c3cc8af8e77e08.
Strike TrickBot_a13af228	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is a13af2286cd59a8963df5feb0a06412e.
Strike TrickBot_a3854599	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is a3854599ec95b48d8aa1e2ad9cb66d16.
Strike TrickBot_a44d2868	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is a44d286885cedd57c317506578337455.
Strike TrickBot_a5cf1da0	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is a5cf1da0e0cf75d265090f3246a73cc1.

<b>Name</b>	<b>Description</b>
Strike TrickBot_a6882fe6	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is a6882fe62b5165f6ec4d64caa7f49448.
Strike TrickBot_a82fc227	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is a82fc227bcfbb5cc79779a5b54982a25.
Strike TrickBot_a8857182	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is a88571827d8203acb046b86406f047fd.
Strike TrickBot_ac9211ce	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is ac9211ced7d9c8915a82fdfe5eda0103.
Strike TrickBot_adc8d3f2	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is adc8d3f293c9fa900655d0550c279c7f.
Strike TrickBot_b3aec372	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is b3aec3723a9c48b96558c15a4e611087.
Strike TrickBot_b6515cc8	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is b6515cc89df6388408ad56d12d496f51.
Strike TrickBot_b951c1df	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is b951c1df23a3735b1351577f3521a876.
Strike TrickBot_bc47b3ab	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is bc47b3ab044ca04355bec9db0649606d.

<b>Name</b>	<b>Description</b>
Strike TrickBot_bd2e3e12	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is bd2e3e12eb604687c5adb105508604d0.
Strike TrickBot_c14c3f99	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has a new section added in the PE file format with random contents. The MD5 hash of this TrickBot sample is c14c3f99bb7182a1cd190f04e9af9c43.
Strike TrickBot_c5983c49	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is c5983c4924d1d5a6810d79f6587aebab.
Strike TrickBot_c71f99ba	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is c71f99ba29dab39e785c5a2b4f82c78c.
Strike TrickBot_c7cbc36f	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is c7cbc36f31fcdf55b87796f18cb009606.
Strike TrickBot_c7e60280	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is c7e6028077e19ff8c82120cd716001f7.
Strike TrickBot_c8d19be2	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is c8d19be28961bb1264baf5bd443404bc.
Strike TrickBot_c8f68051	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is c8f68051462b3f1bd59c4501b9daec3b.

<b>Name</b>	<b>Description</b>
Strike TrickBot_cad58112	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is cad58112e7a1cd4ea253505762e33199.
Strike TrickBot_cafe04d2	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is cafe04d25daaedcb880a433768e0bb96.
Strike TrickBot_cb1f7a9a	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is cb1f7a9a6ce503974b34d8e396fe2e5a.
Strike TrickBot_cb2d2ddd	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is cb2d2ddd9ecaa9f1ca67275d244fc15b.
Strike TrickBot_cce5afd9	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is cce5afd9929ee07858713d32e86253c2.
Strike TrickBot_d04b80a9	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this TrickBot sample is d04b80a9abc3ac86c2a6f9251e41211e.
Strike TrickBot_d13ec5ad	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is d13ec5adc0dae7eb5a0d6cd4fde38af7.
Strike TrickBot_d2f1c8b8	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is d2f1c8b83b13ca3ea422a3ea847f7390.

<b>Name</b>	<b>Description</b>
Strike TrickBot_d813b0f6	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has the checksum removed in the PE file format. The MD5 hash of this TrickBot sample is d813b0f6505f8b1582beb41d3d55d3ae.
Strike TrickBot_ddf00820	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is ddf00820caa8c37f4fc691e6195a3a76.
Strike TrickBot_e06fb6f6	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is e06fb6f69932083d67ec4702520b7210.
Strike TrickBot_e3af376f	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has the debug flag removed in the PE file format. The MD5 hash of this TrickBot sample is e3af376f2df425e0364f9f40bcfe1124.
Strike TrickBot_e4e07dbc	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is e4e07dbc061bbc8f4069eddf0896a23c.
Strike TrickBot_e6931c55	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is e6931c55d71c6678aa050d969c495576.
Strike TrickBot_ec58d221	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is ec58d22179604219c554c56e5551a33a.
Strike TrickBot_ecb155dc	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is ecb155dc156817dcdd3a9e1708f394ba.

<b>Name</b>	<b>Description</b>
Strike TrickBot_ed20b235	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has random bytes appended at the end of the file. The MD5 hash of this TrickBot sample is ed20b2358d873d1699b1af76d15816f2.
Strike TrickBot_ee5900ed	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is ee5900ed3a23bdfe1e47da24b856d1a6.
Strike TrickBot_f06ecf9c	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is f06ecf9c5dc862cd98a8e2ee6f63b286.
Strike TrickBot_f30cc7a6	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this TrickBot sample is f30cc7a6a5d8290c420c2dedf4eebdf7.
Strike TrickBot_f3591383	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this TrickBot sample is f35913834ff4b11ee7971561136d185.
Strike TrickBot_f59c6952	This strike sends a polymorphic malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has the timestamp field updated in the PE file header. The MD5 hash of this TrickBot sample is f59c695229c7b02cf3440338c53dc20.
Strike TrickBot_f9e5b419	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is f9e5b4192366939cbd96afe2d9cfbd41.
Strike TrickBot_ff63ddb4	This strike sends a malware sample known as TrickBot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this TrickBot sample is ff63ddb40ec2e11d7bd734aa4b6f7191.

<b>Name</b>	<b>Description</b>
Strike Trickbot_00dc9c34	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has random bytes appended at the end of the file. The MD5 hash of this Trickbot sample is 00dc9c346cd84fa75d43ccae5bb86c4a.
Strike Trickbot_014f1585	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 014f15859e3ac522851e19e0b2d2786a.
Strike Trickbot_06071333	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Trickbot sample is 06071333ff6320ebdbb5ad09ccace217.
Strike Trickbot_06154c88	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Trickbot sample is 06154c88f3a599cc261ecf19c4c69454.
Strike Trickbot_09277e8a	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has been packed using upx packer, with the default options. The MD5 hash of this Trickbot sample is 09277e8a44f4688f77dd958bb22d4380.
Strike Trickbot_0a92735e	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 0a92735e7370e9c08f1b67480060ef8b.
Strike Trickbot_0ac117ff	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Trickbot sample is 0ac117ff4a3932cb4852872f845359ec.
Strike Trickbot_0fdecaba	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 0fdecabaa0d325922c0330049e68a826.

<b>Name</b>	<b>Description</b>
Strike Trickbot_10047340	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 1004734029c09ec474f332590033643a.
Strike Trickbot_101a4dd4	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 101a4dd4678daafbc91c14a2f9adaec7.
Strike Trickbot_109cfe87	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 109cfe87591896f0e46d896713ff6368.
Strike Trickbot_11364049	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 11364049a6159e255dc03eae0dec6daf.
Strike Trickbot_118d0859	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 118d08599d7b68c09fb4c698d1a6a2f7.
Strike Trickbot_11975ca9	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 11975ca9e9ebb3f66129e59d490fc257.
Strike Trickbot_1238acda	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has random bytes appended at the end of the file. The MD5 hash of this Trickbot sample is 1238acda60f0780986850f48f7dd27a3.
Strike Trickbot_12b50245	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 12b5024549eb5412d5211cf9848b1bfb.

<b>Name</b>	<b>Description</b>
Strike Trickbot_142e8dc7	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 142e8dc74a62a93f3d083925b4c897d3.
Strike Trickbot_186929c3	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 186929c3075e44f6a5dcb92da2c33a33.
Strike Trickbot_1a06cde9	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 1a06cde9178e41846e85627bcf3c2178.
Strike Trickbot_1c70fc8c	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 1c70fc8c8afe9c9d468989442374bc18.
Strike Trickbot_22409c5a	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 22409c5a370a8bb00faace48c76f67fb.
Strike Trickbot_29824072	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 298240723718547126344e86ac09f7d0.
Strike Trickbot_2b8de879	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 2b8de879e137896bf7887a6f26510b01.
Strike Trickbot_2e207b8b	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 2e207b8b85296c23051cd185a936228f.
Strike Trickbot_30559fbf	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 30559fbf94b2a673067d6dfbb21d42c0.

<b>Name</b>	<b>Description</b>
Strike Trickbot_30876c5f	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 30876c5f348002697792091b3ccb7b4a.
Strike Trickbot_31a7a475	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 31a7a4756aeb04493094f0f916eb9f68.
Strike Trickbot_365e7f1d	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 365e7f1dd0f16ca8144cef4bb6543d0b.
Strike Trickbot_3af15873	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 3af158732f544f7c268433efd8d1d486.
Strike Trickbot_3e4fdfbb	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 3e4fdfbb216a4919534246f749aab839.
Strike Trickbot_3f2bda5f	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 3f2bda5f7852cea174cccc8a7e4e1280.
Strike Trickbot_40f7e200	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 40f7e2005a638d80076d9c8b440e8317.
Strike Trickbot_4110c4df	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has been packed using upx packer, with the default options. The MD5 hash of this Trickbot sample is 4110c4dfe514caf5697ae9509b2934c3.

<b>Name</b>	<b>Description</b>
Strike Trickbot_42d57d6e	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 42d57d6e4462240e0995d9deed584047.
Strike Trickbot_439a3893	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 439a38934558b6a2a2d66d9891dc6584.
Strike Trickbot_46b94155	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 46b941555f3008c0a72ae5688f6c1f9b.
Strike Trickbot_4813b76a	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 4813b76a9400b62a0acaab0cb5c09bfe.
Strike Trickbot_4b92c81d	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Trickbot sample is 4b92c81d68490a386f0b75722125c5d9.
Strike Trickbot_625a79a0	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 625a79a068b8b3db62e08db1ec21e7f4.
Strike Trickbot_64a8dfe6	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 64a8dfe64ee1298325a8af441ae6abef.
Strike Trickbot_654b1a59	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 654b1a591b182b0665352dde68720652.

<b>Name</b>	<b>Description</b>
Strike Trickbot_68037c38	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 68037c38f6b16cdf60c8c2b0d29bfeab.
Strike Trickbot_68579257	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Trickbot sample is 68579257c3a277be06202b8568e6dae7.
Strike Trickbot_69f7682d	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 69f7682d754f01aecd9658f57f8670d0.
Strike Trickbot_6b11ef83	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 6b11ef8347c8989e5109e50650282b3b.
Strike Trickbot_713bb022	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 713bb022f264a713db52286227714a58.
Strike Trickbot_72593a33	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 72593a33eada2ecfac60ecf452ccfc1.
Strike Trickbot_76f47ca7	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Trickbot sample is 76f47ca74627e26f8ddfd9add7d9042.
Strike Trickbot_7825d484	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 7825d484da37921be1141cde49d1b9c8.

<b>Name</b>	<b>Description</b>
Strike Trickbot_785973f0	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 785973f0d3f93c1cbc1909bab2b24231.
Strike Trickbot_78896e48	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 78896e48b0e9033f04096ec7eb2a9eee.
Strike Trickbot_7ab7e4b6	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 7ab7e4b69ea3531bb62b2dc2b4b2698e.
Strike Trickbot_81538286	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Trickbot sample is 81538286e9c717293649effac6b84286.
Strike Trickbot_81a23fec	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 81a23fec84b88a2a03d9275e0e234ca4.
Strike Trickbot_81cfada2	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 81cfada27d2a3c2f4e7af0d24803eba.
Strike Trickbot_8a0b7742	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 8a0b7742d05cd9c6b0584c00d6650d79.
Strike Trickbot_90b291b0	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 90b291b0c3e284b4e64072330a8b9f59.

<b>Name</b>	<b>Description</b>
Strike Trickbot_90ef6c70	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 90ef6c70c349f6d735351468b95e2681.
Strike Trickbot_91ff661e	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 91ff661eecc2a978f43dd537ecc40212.
Strike Trickbot_94bedf3b	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 94bedf3bc4df2227f439e7322141fd49.
Strike Trickbot_94e65f4a	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Trickbot sample is 94e65f4a15aacf78dbf61522bc83ed71.
Strike Trickbot_9b902583	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 9b9025830322d872d0ecd63753f1e9b3.
Strike Trickbot_9dfac898	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is 9dfac8989e68abdfda410a3513d9668e.
Strike Trickbot_a1bfc1c4	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is a1bfc1c4c491e866f28d78b88c22e1f2.
Strike Trickbot_a3b99184	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is a3b99184f00044ae955f007961bf68f3.

<b>Name</b>	<b>Description</b>
Strike Trickbot_a40a1b35	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is a40a1b35110eb63c97b6552e8fe765ad.
Strike Trickbot_a67fcd6d	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is a67fcd6db8f635da1bf4fe903199ccc8.
Strike Trickbot_a73478e7	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is a73478e7f62a5856aaed787188c8f777.
Strike Trickbot_a8d9d1a9	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is a8d9d1a932b2afad5a31816cb8b506ca.
Strike Trickbot_a900f134	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is a900f134cca712bb476a37c9ed234f03.
Strike Trickbot_a9392a4d	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is a9392a4d881a556ddf5b4bc812b5e079.
Strike Trickbot_b01b3b95	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has been packed using upx packer, with the default options. The MD5 hash of this Trickbot sample is b01b3b951840d8635e5577f901f1ddb8.
Strike Trickbot_b0bcb4bd	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is b0bcb4bd33305efe3787f572f6c64032.

<b>Name</b>	<b>Description</b>
Strike Trickbot_b1313c41	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is b1313c41c879457c5c15bfefcce64f66.
Strike Trickbot_b638dabc	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is b638dabcf64b3233ea43318c981c536b.
Strike Trickbot_b7a49ceb	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is b7a49ceb3f714dbca3919e75e5428078.
Strike Trickbot_baf6c334	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is baf6c3344d807d2d8e5156c971343feb.
Strike Trickbot_bd704697	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is bd704697b8fce91346d861844017808.
Strike Trickbot_c062e295	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is c062e2956d1d8bfd382bd101289f198b.
Strike Trickbot_c0f61798	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is c0f6179824cdd74331aa36aea17315a3.
Strike Trickbot_c28b0c2c	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary file has one more imports added in the import table. The MD5 hash of this Trickbot sample is c28b0c2ce985e674ee49551f0bd9647b.

<b>Name</b>	<b>Description</b>
Strike Trickbot_c4fb25bb	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has random bytes appended at the end of the file. The MD5 hash of this Trickbot sample is c4fb25bb17180a18dd8bd1cb5097f9bb.
Strike Trickbot_c5382471	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Trickbot sample is c53824718379f0e3cf0844a6ad8cee2a.
Strike Trickbot_c57e344b	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Trickbot sample is c57e344baa928eba318a00f38a934b20.
Strike Trickbot_c5fd8aa7	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is c5fd8aa7309fd0cc9ad0ecaabbeccade.
Strike Trickbot_c771651d	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is c771651d916c8e942c8ebfd7bb0fafc3.
Strike Trickbot_c88c0d52	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is c88c0d5275862ccd9370c7c54e677b0b.
Strike Trickbot_ca0235ca	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is ca0235ca7cf2c01fb3cea65902fa7d1c.
Strike Trickbot_ce9ffaf0	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is ce9ffaf024b3279572607c8512dbd1a0.

<b>Name</b>	<b>Description</b>
Strike Trickbot_d1d23a53	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is d1d23a53b5bf6b060b5714fee99460f2.
Strike Trickbot_d4350a2f	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is d4350a2f7e1cad0ee465f0f8170f8ecf.
Strike Trickbot_d56493d8	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is d56493d83c2260a272e64263f7e17b51.
Strike Trickbot_d91f878b	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is d91f878bc1707aecdb28e895cf5a7fd9.
Strike Trickbot_d9547c4f	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is d9547c4f1c13fac1a1c7e8f8f67df45b.
Strike Trickbot_d9ce38bc	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is d9ce38bc0aeac55de3ee8b579a68e177.
Strike Trickbot_dcb21aee	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is dcbaeef72429aec02c63e9185c9e68.
Strike Trickbot_dd7c7075	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is dd7c70750e4d8dd50603766b1e8aa184.
Strike Trickbot_de14d450	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is de14d450a6ce8140bbd5db0f62e38f94.

<b>Name</b>	<b>Description</b>
Strike Trickbot_e296c4a0	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is e296c4a0cc2e46b055003690dc5c229c.
Strike Trickbot_e2ff2674	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is e2ff26741a46499b6e5eb4b0b9786b2a.
Strike Trickbot_e4751c1f	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Trickbot sample is e4751c1f57c370d74ef96f814c1a1b06.
Strike Trickbot_e526b5b1	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is e526b5b1a4d463faec53a88294345d62.
Strike Trickbot_e5d84074	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is e5d84074f043e53fc6f74e3bc2b4017.
Strike Trickbot_ea8ace01	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is ea8ace0142ab9a30a140134d558a43df.
Strike Trickbot_ef04159c	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is ef04159c8fe8e551672f0a47425aa5a3.
Strike Trickbot_f41121eb	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Trickbot sample is f41121eb8348e32778f16d1866a71409.

<b>Name</b>	<b>Description</b>
Strike Trickbot_f8a79cd8	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is f8a79cd887e6074e77e258bdd86f6913.
Strike Trickbot_fae34a61	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is fae34a61be4d7b2f15de7e8aaad8358b.
Strike Trickbot_fb145828	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is fb145828b548f5c3c20c4fe985bd969.
Strike Trickbot_fc0c2d9d	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is fc0c2d9dc18806606d6e2673db4380a.
Strike Trickbot_fe4d51a8	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is fe4d51a8e7b27afedd8cca6e894b7aab.
Strike Trickbot_ffed0c2a	This strike sends a malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The MD5 hash of this Trickbot sample is ffed0c2a620dee39b6ea0148189a291a.
Strike Trickbot_ffeec37f	This strike sends a polymorphic malware sample known as Trickbot. Trickbot is a banking trojan targeting sensitive information for select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts. The binary has been packed using upx packer, with the default options. The MD5 hash of this Trickbot sample is ffeec37f8f562ecddf5c61ca964e8a28.
Strike Triton RAT_0bcc0bf	This strike sends a malware sample known as Triton RAT. Triton RAT is a Python Remote Access Trojan that uses Telegram to allow a user to gain remote control of a system. This RAT provides the ability to execute remote commands, steal Roblox security cookies, steal clipboard data and perform many other functions. The MD5 hash of this Triton RAT sample is 0bcc0bf09da84e0afa139e8fa50f5e6.

<b>Name</b>	<b>Description</b>
Strike Triton RAT_0ea83f25	This strike sends a malware sample known as Triton RAT. Triton RAT is a Python Remote Access Trojan that uses Telegram to allow a users gain remote control of a system. This RAT provides the ability to execute remote commands, steal Roblox security cookies, steal clipboard data and perform many other functions. The MD5 hash of this Triton RAT sample is 0ea83f256e4bedf7269bc1a0102d8d76.
Strike Triton RAT_9b17269a	This strike sends a malware sample known as Triton RAT. Triton RAT is a Python Remote Access Trojan that uses Telegram to allow a users gain remote control of a system. This RAT provides the ability to execute remote commands, steal Roblox security cookies, steal clipboard data and perform many other functions. The MD5 hash of this Triton RAT sample is 9b17269a5845e3d49d4886645c887a94.
Strike Triton RAT_cf94873d	This strike sends a malware sample known as Triton RAT. Triton RAT is a Python Remote Access Trojan that uses Telegram to allow a users gain remote control of a system. This RAT provides the ability to execute remote commands, steal Roblox security cookies, steal clipboard data and perform many other functions. The MD5 hash of this Triton RAT sample is cf94873df58eadaa69915337eecc3857.
Strike Triton RAT_dde70806	This strike sends a malware sample known as Triton RAT. Triton RAT is a Python Remote Access Trojan that uses Telegram to allow a users gain remote control of a system. This RAT provides the ability to execute remote commands, steal Roblox security cookies, steal clipboard data and perform many other functions. The MD5 hash of this Triton RAT sample is dde70806e58f2e9ed6cdbe275ae18097.
Strike Triton RAT_f34b340d	This strike sends a malware sample known as Triton RAT. Triton RAT is a Python Remote Access Trojan that uses Telegram to allow a users gain remote control of a system. This RAT provides the ability to execute remote commands, steal Roblox security cookies, steal clipboard data and perform many other functions. The MD5 hash of this Triton RAT sample is f34b340d5d85f405f1d28ac00a9b938f.
Strike TrollAgent_7457dc03	This strike sends a malware sample known as TrollAgent. TrollAgent is a GoLang-based infostealer malware that masquerades as a legitimate security program. Two types of malware strains are installed through this process - one is a backdoor malware that receives the threat actor's commands externally to perform various malicious activities, and an infostealer that collects information from the infected systems. The MD5 hash of this TrollAgent sample is 7457dc037c4a5f3713d9243a0dfb1a2c.
Strike TrollAgent_87429e92	This strike sends a malware sample known as TrollAgent. TrollAgent is a GoLang-based infostealer malware that masquerades as a legitimate security program. Two types of malware strains are installed through this process - one is a backdoor malware that receives the threat actor's commands externally to perform various malicious activities, and an infostealer that collects information from the infected systems. The MD5 hash of this TrollAgent sample is 87429e9223d45e0359cd1c41c0301836.
Strike TrollAgent_88f18330	This strike sends a malware sample known as TrollAgent. TrollAgent is a GoLang-based infostealer malware that masquerades as a legitimate security program. Two types of malware strains are installed through this process - one is a backdoor malware that receives the threat actor's commands externally to perform various malicious activities, and an infostealer that collects information from the infected systems. The MD5 hash of this TrollAgent sample is 88f183304b99c897aacfa321d58e1840.

<b>Name</b>	<b>Description</b>
Strike TrollAgent_a67cf9ad	This strike sends a malware sample known as TrollAgent. TrollAgent is a GoLang-based infostealer malware that masquerades as a legitimate security program. Two types of malware strains are installed through this process - one is a backdoor malware that receives the threat actor's commands externally to perform various malicious activities, and an infostealer that collects information from the infected systems. The MD5 hash of this TrollAgent sample is a67cf9add2905c11f5c466bc01d554b0.
Strike TrollAgent_c8e7b0d3	This strike sends a malware sample known as TrollAgent. TrollAgent is a GoLang-based infostealer malware that masquerades as a legitimate security program. Two types of malware strains are installed through this process - one is a backdoor malware that receives the threat actor's commands externally to perform various malicious activities, and an infostealer that collects information from the infected systems. The MD5 hash of this TrollAgent sample is c8e7b0d3b6afa22e801cacaf16b37355.
Strike Troll_Stealer_77405619	This strike sends a malware sample known as Troll Stealer. Troll Stealer is a Go based information stealer with ties to the GoBear and BetaSeed backdoors. It can retrieve various information from the system like SSH credentials, files and directories, screen captures and send it back via C2 communication. The MD5 hash of this Troll Stealer sample is 77405619a2201134cf900ef74f072af8.
Strike Troll_Stealer_9e75705b	This strike sends a malware sample known as Troll Stealer. Troll Stealer is a Go based information stealer with ties to the GoBear and BetaSeed backdoors. It can retrieve various information from the system like SSH credentials, files and directories, screen captures and send it back via C2 communication. The MD5 hash of this Troll Stealer sample is 9e75705b4930f50502bcbd740fc3ece1.
Strike Tycoon_12a47095	This strike sends a malware sample known as Tycoon. Tycoon is a multi-platform Java-based ransomware which targets Windows and Linux systems. The ransomware attempts to infiltrate small to medium sized companies and institutions in education and software industries The MD5 hash of this Tycoon sample is 12a470956f7437a00d7bcf47f1995ea7.
Strike Tycoon_51a7822f	This strike sends a malware sample known as Tycoon. Tycoon is a multi-platform Java-based ransomware which targets Windows and Linux systems. The ransomware attempts to infiltrate small to medium sized companies and institutions in education and software industries The MD5 hash of this Tycoon sample is 51a7822f388162ce1c66dd90da207545.
Strike Tycoon_80675f08	This strike sends a malware sample known as Tycoon. Tycoon is a multi-platform Java-based ransomware which targets Windows and Linux systems. The ransomware attempts to infiltrate small to medium sized companies and institutions in education and software industries The MD5 hash of this Tycoon sample is 80675f08a4dad40a316865619f6adaaa.
Strike Tycoon_9c7befb1	This strike sends a malware sample known as Tycoon. Tycoon is a multi-platform Java-based ransomware which targets Windows and Linux systems. The ransomware attempts to infiltrate small to medium sized companies and institutions in education and software industries The MD5 hash of this Tycoon sample is 9c7befb18ccbd63100a497fe7c1acc69.

<b>Name</b>	<b>Description</b>
Strike Tycoon_ae037348	This strike sends a malware sample known as Tycoon. Tycoon is a multi-platform Java-based ransomware which targets Windows and Linux systems. The ransomware attempts to infiltrate small to medium sized companies and institutions in education and software industries The MD5 hash of this Tycoon sample is ae03734805e3b7ec0fa52c5a4f07a725.
Strike Tycoon_b58476f6	This strike sends a malware sample known as Tycoon. Tycoon is a multi-platform Java-based ransomware which targets Windows and Linux systems. The ransomware attempts to infiltrate small to medium sized companies and institutions in education and software industries The MD5 hash of this Tycoon sample is b58476f659782f770854726847601fda.
Strike Tycoon_d3f44bfe	This strike sends a malware sample known as Tycoon. Tycoon is a multi-platform Java-based ransomware which targets Windows and Linux systems. The ransomware attempts to infiltrate small to medium sized companies and institutions in education and software industries The MD5 hash of this Tycoon sample is d3f44bfe42b2e3c735e9df5bb793b9ef.
Strike Tycoon_f28c603b	This strike sends a malware sample known as Tycoon. Tycoon is a multi-platform Java-based ransomware which targets Windows and Linux systems. The ransomware attempts to infiltrate small to medium sized companies and institutions in education and software industries The MD5 hash of this Tycoon sample is f28c603bbe75516372159bb79ef3eb63.
Strike UAC-0057_0767b2a1	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 0767b2a1b9c596ec1865440e71b88f2d.
Strike UAC-0057_1520993f	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 1520993f3ad3bc307a40e7e056d364cb.
Strike UAC-0057_1541d989	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 1541d989d8908b55d7a08d3683579027.

<b>Name</b>	<b>Description</b>
Strike UAC-0057_38580294	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 38580294995d09e2ceacaf17fb03d609.
Strike UAC-0057_408d3148	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 408d3148fbb750a9c0b0e3c4a6017d67.
Strike UAC-0057_47c1349e	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 47c1349ec74f11b5b17de51ede1c5ec7.
Strike UAC-0057_5389e211	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 5389e211ec37519039d6aea8851a6254.
Strike UAC-0057_60fc5ef9	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 60fc5ef9e8de4b663cf2c38e040f4ac0.

<b>Name</b>	<b>Description</b>
Strike UAC-0057_65a7afe1	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 65a7afe1af0fe1ef78af70267e01fff4.
Strike UAC-0057_75af8b50	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 75af8b50c5939b4186108d0ac24a9cdc.
Strike UAC-0057_7c202bc0	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 7c202bc012974783beacf526409f30d8.
Strike UAC-0057_8c4f881c	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is 8c4f881c12957b8e581ef7e97a61f109.
Strike UAC-0057_b63d0634	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is b63d0634d5497320ded7bea7a507b26e.

<b>Name</b>	<b>Description</b>
Strike UAC-0057_c5f60a8e	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is c5f60a8ea7b1ea50962f14d5291a56f1.
Strike UAC-0057_cfed77c8	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is cfed77c806dffaa7b48a17f9bc2b68bf4.
Strike UAC-0057_e21f3104	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is e21f310442347eed2210a75c1fa8e01.
Strike UAC-0057_e5830a1e	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is e5830a1ee8791d16939d95183a360c99.
Strike UAC-0057_eec3f959	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is eec3f9594965066db8aa5482e18618bd.

<b>Name</b>	<b>Description</b>
Strike UAC-0057_f7ca2539	This strike sends a malware sample known as UAC-0057. UAC-0057 is a malware, specifically a Trojan, that targets organizations in Ukraine and Poland. It is delivered via phishing emails with malicious Microsoft Excel attachments that contain a VBA macro. Once the macro is enabled, it downloads and executes the malware from a remote server. Its key capabilities include stealing system information, executing commands remotely, and downloading additional malware or updates from the command and control server. The MD5 hash of this UAC-0057 sample is f7ca25396926c6b7c35f9c86d9f79f36.
Strike UAT-8099_012dd968	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 012dd9682230ce26aefa84a9d75bedbc.
Strike UAT-8099_24762276	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 24762276a8f080a6e6d77bea05385f91.
Strike UAT-8099_34114faa	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 34114faa30feb8dabc8074646c8c7937.
Strike UAT-8099_37ca2f20	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 37ca2f2065f79f5b718d5e55f7dabb8e.

<b>Name</b>	<b>Description</b>
Strike UAT-8099_3d880c3f	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 3d880c3f1325c6d9dd7cb97c8e2180ab.
Strike UAT-8099_551c7a45	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 551c7a45ee57e666c2e1655845958db6.
Strike UAT-8099_841a5272	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 841a5272bfb67cf4c56c086e07601005.
Strike UAT-8099_97791d41	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is 97791d414cb9e442934adae3958424e2.
Strike UAT-8099_d30b2b33	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is d30b2b33998d2498c983bfde1b99a76e.

<b>Name</b>	<b>Description</b>
Strike UAT-8099_db4e8d99	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is db4e8d990cb9d6ec06ad47c2311e3701.
Strike UAT-8099_ee127dbe	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is ee127dbe8daa25640c2501004f1547b0.
Strike UAT-8099_f30db5d9	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is f30db5d99477f0d2ffa2f8b578c6f1d1.
Strike UAT-8099_f79e154b	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is f79e154b77a248493bc4d34ea1c19547.
Strike UAT-8099_f9f87fcf	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is f9f87fcfd6ecc6d65381f97aec65f75b.

<b>Name</b>	<b>Description</b>
Strike UAT-8099_fef21f73	This strike sends a malware sample known as UAT-8099. UAT-8099 is a malware of the Remote Access Trojan (RAT) family that is used by a Chinese hacker group to conduct SEO fraud. The malware is delivered through malicious SEO-optimized web pages that trick users into downloading it. Once executed, UAT-8099 establishes a backdoor into the victim's system, allowing the attacker to gain unauthorized access. Key capabilities of this malware include the ability to execute arbitrary commands, manipulate files and processes, and steal sensitive data. The MD5 hash of this UAT-8099 sample is fef21f73ba6da0cb6221976a8fb64cdd.
Strike Upatre_0c1a60cc	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 0c1a60cc41945330782daf847ffea289.
Strike Upatre_0db48119	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 0db48119cb0a09eefdfa8f8ae7d2a114.
Strike Upatre_12b8dbba	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 12b8dbbacf6c077b871ae1c699abbf8b.
Strike Upatre_14b99208	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 14b99208c98f98a9ee76b5f9d3eef207.
Strike Upatre_16ada888	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 16ada888c2f3bd7b9c00ff446dda9dc5.
Strike Upatre_1914a94c	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 1914a94cbf4c339109e360bd7c9e3bdf.
Strike Upatre_1ba36e0d	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 1ba36e0dd3b26bce1b1c9dabefb4fa96.
Strike Upatre_1f762ed0	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 1f762ed0c7ae10472ebd1652a5726664.

<b>Name</b>	<b>Description</b>
Strike Upatre_1fecaffb	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 1fecaffb77c73960b7fd8e8b5106fa27.
Strike Upatre_2784f9de	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 2784f9de40228cb4e33fcb9087272b61.
Strike Upatre_388509bf	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 388509bfd329230b16e57ddd0c644782.
Strike Upatre_39642987	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 396429877506a4ffef0afeb47e9b3ffd.
Strike Upatre_3affcb33	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 3affcb33be9245925725fac356b626c7.
Strike Upatre_3d374745	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 3d3747456ab3054f941ec41ebdc3ef1b.
Strike Upatre_436d40ee	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 436d40eec22ddf5acf2487a3a12b3741.
Strike Upatre_45df574c	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 45df574c429c134460b49582c8d58b9c.
Strike Upatre_516aca8d	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 516aca8d0b9a6bd8fe6364a5b11b4795.
Strike Upatre_563bb276	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 563bb2763d7d88c90ad31160e34c3987.

<b>Name</b>	<b>Description</b>
Strike Upatre_5954c22b	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 5954c22bbc31a84fcbd8d2c52cc5e584.
Strike Upatre_59c88af4	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 59c88af4fe326e03a831137f42e1a052.
Strike Upatre_5afd1fc4	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 5afd1fc4afa9839e10360f9fc226c7f1.
Strike Upatre_5edf7db2	This strike sends a polymorphic malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Upatre sample is 5edf7db2bd5a1fab86a8578cdb9a59f9.
Strike Upatre_601800e9	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 601800e912ba03a97c3a70fadd1a31db.
Strike Upatre_64a1ac87	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 64a1ac8768ffaac0eb6244710df52337.
Strike Upatre_6533365d	This strike sends a polymorphic malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The binary has random bytes appended at the end of the file. The MD5 hash of this Upatre sample is 6533365d6f92c906024674cb558d45b3.
Strike Upatre_6696c125	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 6696c125bcd1826b0d722e57358259c.
Strike Upatre_69e7c2a4	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 69e7c2a49d3fb406e48f5d8c7c1a5a0e.
Strike Upatre_7df2152c	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 7df2152c90d5602f7f699963f22d53ec.

<b>Name</b>	<b>Description</b>
Strike Upatre_80107b79	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 80107b7966dc8623b34119eeb4544fc2.
Strike Upatre_810a21a6	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 810a21a6625558dbab76edbaff8052c0.
Strike Upatre_83392327	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 8339232735ecae5963462f7c4e73ef85.
Strike Upatre_8bd23683	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 8bd23683d0dbe54d9eb28015754fb5d.
Strike Upatre_8df21c17	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 8df21c177228404e4b420b9753f10f14.
Strike Upatre_93b55474	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 93b5547485c011752b3a7320bc12c31f.
Strike Upatre_9442a6f1	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 9442a6f1fd43df3f583e2aabbb0f96e8.
Strike Upatre_94badbce	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 94badbcede0d0f8c50cca6a841c2eb40.
Strike Upatre_94e8ab9f	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 94e8ab9fbe70de0fcc8b90b6125ff060.
Strike Upatre_9547e2c9	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 9547e2c96ca9870c05e12cce16bd244f.

<b>Name</b>	<b>Description</b>
Strike Upatre_9b764435	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 9b764435ddc3f80e8a2d02d1a6645d20.
Strike Upatre_9bc218bb	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is 9bc218bb7b56b26ccf4e6bbdf45459f5.
Strike Upatre_a1c85d50	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is a1c85d50e3102a36da4d5d5d0b00a0dd.
Strike Upatre_acdac2c5	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is acdac2c5775617d2862fd45cf700f75a.
Strike Upatre_b1de5235	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is b1de5235a3e3429f25828979ddf0be7.
Strike Upatre_b6c86a0d	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is b6c86a0d0948e4b9229a159ed92c4f11.
Strike Upatre_bc395d0d	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is bc395d0d7aef73b9efd9e5cceebc1e7f.
Strike Upatre_bef65556	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is bef65556114fb20ab24c2bd4537d077c.
Strike Upatre_c3e570fc	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is c3e570fc670c2c76e36a072f06740bd4.
Strike Upatre_c91bbae0	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is c91bbae0a5801481cdb662aad812b01b.

<b>Name</b>	<b>Description</b>
Strike Upatre_d481d1cc	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is d481d1ccafdaec0da47049d151459e4e.
Strike Upatre_d515ca49	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is d515ca498c35f7103fc2618ca68df3f1.
Strike Upatre_d653f929	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is d653f92976cacce962b17817f52012f1.
Strike Upatre_d6ec3e39	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is d6ec3e39ce013ea0a2ea573d90445ff8.
Strike Upatre_e02e8b78	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is e02e8b78d91f0c16cd7b6a0dea93353a.
Strike Upatre_e3366e0c	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is e3366e0c6698189b4315e6fd9fd087c2.
Strike Upatre_f0256ed3	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is f0256ed39ffdd70c0df59941538d041b.
Strike Upatre_f2178ed2	This strike sends a malware sample known as Upatre. Upatre is a malicious downloader often used by exploit kits and phishing campaigns. Upatre downloads and executes malicious executables, such as banking malware. The MD5 hash of this Upatre sample is f2178ed21d3fa0e4d3c9e864365d5a63.
Strike Ursnif_91debc88	This strike sends a malware sample known as Ursnif. Ursnif is used to steal sensitive information from an infected host and can also act as a malware downloader. It is commonly spread through malicious emails or exploit kits. The MD5 hash of this Ursnif sample is 91debc889c24d97edeab1c65810b239c.
Strike Ursnif_9201b26c	This strike sends a malware sample known as Ursnif. Ursnif is used to steal sensitive information from an infected host and can also act as a malware downloader. It is commonly spread through malicious emails or exploit kits. The MD5 hash of this Ursnif sample is 9201b26ca98c8cf301348e64dab51c13.

<b>Name</b>	<b>Description</b>
Strike VHD_2d5da841	This strike sends a polymorphic malware sample known as VHD. The binary has a random section name renamed according to the PE format specification. VHD is believed to be a high profile targeted ransomware owned and operated by the Lazarus Group. It encrypts all files on connected devices and deletes folders named "System Volume Information". The program also employs some interesting techniques such as, the ability to stop processes that could be locking important files, a mechanism to resume operations if the encryption process is interrupted, and it's copied and executed through WMI calls. The MD5 hash of this VHD sample is 2d5da841280f2544e0516cfb40f2a0a9.
Strike VHD_ccc6026a	This strike sends a malware sample known as VHD. VHD is believed to be a high profile targeted ransomware owned and operated by the Lazarus Group. It encrypts all files on connected devices and deletes folders named "System Volume Information". The program also employs some interesting techniques such as, the ability to stop processes that could be locking important files, a mechanism to resume operations if the encryption process is interrupted, and it's copied and executed through WMI calls. The MD5 hash of this VHD sample is ccc6026acf7eadada9adaccab70ca4d6.
Strike VHD_dd00a861	This strike sends a malware sample known as VHD. VHD is believed to be a high profile targeted ransomware owned and operated by the Lazarus Group. It encrypts all files on connected devices and deletes folders named "System Volume Information". The program also employs some interesting techniques such as, the ability to stop processes that could be locking important files, a mechanism to resume operations if the encryption process is interrupted, and it's copied and executed through WMI calls. The MD5 hash of this VHD sample is dd00a8610bb84b54e99ae8099db1fc20.
Strike VHD_e29a03db	This strike sends a polymorphic malware sample known as VHD. The binary has random contents appended in one of the existing sections in the PE file format. VHD is believed to be a high profile targeted ransomware owned and operated by the Lazarus Group. It encrypts all files on connected devices and deletes folders named "System Volume Information". The program also employs some interesting techniques such as, the ability to stop processes that could be locking important files, a mechanism to resume operations if the encryption process is interrupted, and it's copied and executed through WMI calls. The MD5 hash of this VHD sample is e29a03dbec644238fa5257311d428694.
Strike VHD_efd4a87e	This strike sends a malware sample known as VHD. VHD is believed to be a high profile targeted ransomware owned and operated by the Lazarus Group. It encrypts all files on connected devices and deletes folders named "System Volume Information". The program also employs some interesting techniques such as, the ability to stop processes that could be locking important files, a mechanism to resume operations if the encryption process is interrupted, and it's copied and executed through WMI calls. The MD5 hash of this VHD sample is efd4a87e7c5dcbb64b7313a13b4b1012.

<b>Name</b>	<b>Description</b>
Strike VHD_fa1f20d9	This strike sends a polymorphic malware sample known as VHD. The binary has random bytes appended at the end of the file. VHD is believed to be a high profile targeted ransomware owned and operated by the Lazarus Group. It encrypts all files on connected devices and deletes folders named "System Volume Information". The program also employs some interesting techniques such as, the ability to stop processes that could be locking important files, a mechanism to resume operations if the encryption process is interrupted, and it's copied and executed through WMI calls. The MD5 hash of this VHD sample is fa1f20d928ae60a5dedcd3522dde2252.
Strike ValleyFall_027d0cc7	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 027d0cc7b56355543cc2e205b0b11377.
Strike ValleyFall_0a0ae655	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 0a0ae6554670f2a4dfbc929aca5dedec.
Strike ValleyFall_11fc1bf8	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 11fc1bf831cb3bc57d3ff15080575f8a.
Strike ValleyFall_1539d1f4	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 1539d1f4c573d787e07ddc605caf450.
Strike ValleyFall_1d68af9d	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 1d68af9dc752856b0c403efffac46c8.
Strike ValleyFall_240dd7e9	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 240dd7e9a40543128dd29a8e3344a6ff.

<b>Name</b>	<b>Description</b>
Strike ValleyFall_24c1507e	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 24c1507ed75561261069ad6df6581e65.
Strike ValleyFall_265446b5	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 265446b5f00447fb1f381dca10dfbcd1.
Strike ValleyFall_26ed6272	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 26ed6272d2763bef12343fd4787923b1.
Strike ValleyFall_27c50fd3	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 27c50fd30006985e87db28b3f7ef39b3.
Strike ValleyFall_2cc68018	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 2cc68018d8cb892c68d84833b29b6789.
Strike ValleyFall_2d422e29	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 2d422e299f474a2df7b0db9059405753.
Strike ValleyFall_35018174	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 3501817402fb055a95a8de90663fdb15.
Strike ValleyFall_3984ad4a	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 3984ad4a451da991f87757a1619b2982.

<b>Name</b>	<b>Description</b>
Strike ValleyFall_39970f25	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 39970f254b9b88a8879ce5322c6112a9.
Strike ValleyFall_3e234685	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 3e234685b6b56540779171b01b1cd50d.
Strike ValleyFall_40ba5430	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 40ba5430393670e09d9ddad5b7fb8b79.
Strike ValleyFall_432ee8f4	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 432ee8f47e135944e76df8a69a4ecdb7.
Strike ValleyFall_4a36493f	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 4a36493f7c8f9cdf791494ba8dd5a722.
Strike ValleyFall_4e0eede2	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 4e0eede2ec64e94d200a10ad5e90c456.
Strike ValleyFall_5eb8a9ae	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 5eb8a9ae66235bbb3f356760742975bb.
Strike ValleyFall_6055c3ab	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 6055c3aba10b4cef55c4b007c7097a34.

<b>Name</b>	<b>Description</b>
Strike ValleyFall_6136baea	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 6136baea95458c0600ce74c1eda38a0e.
Strike ValleyFall_65f3fee2	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 65f3fee27d0a0d041dd3db534b5cc831.
Strike ValleyFall_6d62b0ea	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 6d62b0ea7485bd3fb78054bf4ae1d29e.
Strike ValleyFall_7818811b	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 781881bb3842ce5cdc17e5143fc947.
Strike ValleyFall_793bb9a6	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 793bb9a6e946d296ee80e5cc7d12f58f.
Strike ValleyFall_79479b19	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 79479b19ce3b927609ef21f4ff21f5fb.
Strike ValleyFall_7b6cd562	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 7b6cd562aa414a779f129f7d979a86d4.
Strike ValleyFall_7c123e51	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 7c123e5142990f1ae07cb4ed0bd1710c.

<b>Name</b>	<b>Description</b>
Strike ValleyFall_7c2d7b1a	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 7c2d7b1ac2274105195b397b28510bd6.
Strike ValleyFall_80397e97	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 80397e978a79758ffb9bd0e05a5b4227.
Strike ValleyFall_8161ef8c	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 8161ef8c40202f37d9f83093851aeed7.
Strike ValleyFall_81f05061	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 81f05061c87f756b8c0059c45e0fc3f6.
Strike ValleyFall_885189cf	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 885189cf7269d6abc2590e06c14178d9.
Strike ValleyFall_8bbb493c	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 8bbb493c03fb17a691f896f91d753b6f.
Strike ValleyFall_8c07ed8c	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is 8c07ed8cd7666c73fdf8e4c9d08d8e53.
Strike ValleyFall_a34557c2	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is a34557c25044b9dd1df9c5a404895386.

<b>Name</b>	<b>Description</b>
Strike ValleyFall_a5379184	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is a5379184d39eebe51edb5a1dd8ee5c35.
Strike ValleyFall_a6390f90	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is a6390f906aedcd3ebc04ca12a5a7a118.
Strike ValleyFall_a823c02d	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is a823c02d7a4a81f1205e35aa6ef6f456.
Strike ValleyFall_a9a419af	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is a9a419af6c98f7f8b68e84d1fe48c037.
Strike ValleyFall_b3e30cdf	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is b3e30cdf9d4ea5e4499068929fed6ae0.
Strike ValleyFall_b639f411	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is b639f4119976f944a90cb5c92b4c7bb3.
Strike ValleyFall_bc2fcde7	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is bc2fcde71ea7965d0de6a615eab7c4b4.
Strike ValleyFall_bcf4561c	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is bcf4561c11d9110f937e0b0ffc6f1a6a.

<b>Name</b>	<b>Description</b>
Strike ValleyFall_c47654f8	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is c47654f89f889c5e6834047281e88865.
Strike ValleyFall_c78dfe66	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is c78dfe66b3f6c1cc83837fd5ae71e780.
Strike ValleyFall_cbd6b4b0	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is cbd6b4b00ce7f93e408467522164d460.
Strike ValleyFall_d82397fb	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is d82397ffb236c86fdd352c86b4871045.
Strike ValleyFall_dbe43b01	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is dbe43b01c4ffa6423b8032048006ec0.
Strike ValleyFall_dfdb7466	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is dfdb74665f7d7815a2a2d48b6a19ebd6.
Strike ValleyFall_e21cf4c	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is e21cf4c63ca75d73997f7a2c12ac412.
Strike ValleyFall_e4ff1e73	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is e4ff1e73fe600fce7fee214d9baeb6a6.

<b>Name</b>	<b>Description</b>
Strike ValleyFall_e6cab789	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is e6cab789649fc15ff44880a5ba603dd8.
Strike ValleyFall_e75f00bf	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is e75f00bfbbbaa72b44532eae3fcf4fc20.
Strike ValleyFall_ecfcaa80	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is ecfcaa803a8eb31dfec1931bab0aca1d.
Strike ValleyFall_efb542d0	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is efb542d0533096bca030783dd1b36eb7.
Strike ValleyFall_f02b5ec6	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is f02b5ec67be091cc1aa89f3243226bc7.
Strike ValleyFall_f4d3df59	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is f4d3df5955578f51d309973c313bfea2.
Strike ValleyFall_f7e69655	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is f7e69655a6ca7f3d2685bf3da7c4f309.
Strike ValleyFall_fb569c4f	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is fb569c4f113f44f6db78385daae8a673.

<b>Name</b>	<b>Description</b>
Strike ValleyFall_fb8cb88cb	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is fb8cb88cb1e358d57c0a43cb4cc6f977f.
Strike ValleyFall_fc4d6f3e	This strike sends a malware sample known as ValleyFall. ValleyFall is spyware that was discovered in April 2023. The malware has the ability to perform many functions like keylogging, gathering data, listing system process, downloading and executing files, and communicating with an external C2 server. It also tries to evade analysis by performing system process scans. The MD5 hash of this ValleyFall sample is fc4d6f3e43d2fe99f680c0c5404591c4.
Strike Valyria_7a99e31e	This strike sends a malware sample known as Valyria. Valyria is a malicious Microsoft Word document family that is used to distribute other malware. This campaign is currently spreading Emotet. The MD5 hash of this Valyria sample is 7a99e31edacad7d23cc718347fdb4558.
Strike Vatet Loader_039e75cd	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 039e75cdd8787394789d11ca6d2c7711.
Strike Vatet Loader_05d24dd8	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 05d24dd80b9a39e2148e94c742f8f16b.
Strike Vatet Loader_088d29b4	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 088d29b4a238a650e12f5ce97ec58289.
Strike Vatet Loader_0ea9b7a2	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 0ea9b7a283e7d4601fb7dbd63493b342.

<b>Name</b>	<b>Description</b>
Strike Vatet Loader_13cc74a4	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 13cc74a4168aab6c63b5e44358f47604.
Strike Vatet Loader_164b162f	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 164b162f8cd59acf9d3da0bec7ea1c52.
Strike Vatet Loader_1d191d54	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 1d191d54cdd3adb4621b5c3a13d1ea91.
Strike Vatet Loader_1f937cba	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 1f937cbae354345087860c7d33e0e61d.
Strike Vatet Loader_2133b1c7	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 2133b1c7bb6145cdd121eb8c423d35a7.
Strike Vatet Loader_225747a3	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 225747a368357a5eafaac5337ee56c9a.
Strike Vatet Loader_23594ad0	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 23594ad0ba8ec37ad5eaec84aee9cecd.

<b>Name</b>	<b>Description</b>
Strike Vatet Loader_23dae475	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 23dae47577cda08dfc82e65e1217cbee.
Strike Vatet Loader_25e8d46d	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 25e8d46d27e0a1034804aba00ba75d38.
Strike Vatet Loader_26e4a744	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 26e4a7443332461d330e6dc4e9a22f5b.
Strike Vatet Loader_2f634065	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 2f6340654f5d07c7a5d19b9d228dabb1.
Strike Vatet Loader_31dc5267	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 31dc5267d3daf057baaa37f8d5d59229.
Strike Vatet Loader_41eff4cd	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 41eff4cd049a8b5debf437b229e7c044.
Strike Vatet Loader_4b3064c2	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 4b3064c24cb16361027233138fd539dc.

<b>Name</b>	<b>Description</b>
Strike Vatet Loader_4bee8553	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 4bee85530d15be0a9e6c8672e355ddc6.
Strike Vatet Loader_4d1b52e3	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 4d1b52e30629477a12dcf2bbbc196e88.
Strike Vatet Loader_4ef81756	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 4ef817562dc042e616ae26a2c8773f23.
Strike Vatet Loader_4f2c11ee	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 4f2c11ee45ce87eeee7789b43cc91ac3.
Strike Vatet Loader_615292e1	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 615292e183cf11759b672148998bfa18.
Strike Vatet Loader_6363cba1	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 6363cba1430bf8a617d789b49e275975.
Strike Vatet Loader_643fbcd4	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 643fbcd40041c2b57a2740bb02e16db0.

<b>Name</b>	<b>Description</b>
Strike Vatet Loader_68cb520d	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 68cb520d2084020638790187e34638ea.
Strike Vatet Loader_6932dfcd	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 6932dfcd3789f88e828d939174183446.
Strike Vatet Loader_6f6a04e6	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 6f6a04e60af90862b2ced5864b6b23f9.
Strike Vatet Loader_7031a113	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 7031a1138e1892fb09bfbd518dba07b.
Strike Vatet Loader_77e9031a	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 77e9031a6ba4afeecda915e914a352df.
Strike Vatet Loader_80419652	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 8041965231306e1c2dff3695d6327524.
Strike Vatet Loader_808c9568	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 808c956808d1a47b50f51df08d45f391.

Name	Description
Strike Vatet Loader_81ba4107	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 81ba4107943bb4ad2ec351ba2417f987.
Strike Vatet Loader_94b27b9d	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 94b27b9de692308cdb07aa6cc31391f1.
Strike Vatet Loader_988b54d6	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 988b54d62c2163cdb5398ff6571e3c80.
Strike Vatet Loader_99354355	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 9935435529057201dac86957275a43e9.
Strike Vatet Loader_9d4c4af4	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is 9d4c4af4b600bb90e92a5c0b86551507.
Strike Vatet Loader_aa0bf004	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is aa0bf0045c4faa988815117cebcacdeb.
Strike Vatet Loader_ae07f0b1	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is ae07f0b180bc52b39000f50353e4e97d.

<b>Name</b>	<b>Description</b>
Strike Vatet Loader_b18ee982	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is b18ee982de606adc6715e7a52648b63c.
Strike Vatet Loader_b5d6214c	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is b5d6214c223b3f6bc4a77c47e0e2a864.
Strike Vatet Loader_b90fbb7a	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is b90fbb7ae572eca2f64d14c0e0dc4a21.
Strike Vatet Loader_c7e84d5c	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is c7e84d5c86f51a349445ad126c42fd89.
Strike Vatet Loader_ca4682a3	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is ca4682a32cdaaf2c0357a2a79e32ee9b.
Strike Vatet Loader_dba03b64	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is dba03b64b963b77fe966238c261aace4.
Strike Vatet Loader_dcba8d6c	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is dcba8d6cf6b336ac96db500ad99b0013.

Name	Description
Strike Vatet Loader_ddf9e951	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is ddf9e95123d9b585fa9e164236bfd338.
Strike Vatet Loader_e0d2c9aa	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is e0d2c9aac9a8489a2154aff6e0abcb6e.
Strike Vatet Loader_e2b15234	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is e2b15234dee641b74ee7959df2ae2e43.
Strike Vatet Loader_e5b622b9	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is e5b622b9864d3a2e31a4edac46c1cb0c.
Strike Vatet Loader_e843170e	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is e843170e564321228fc88b9291a4265c.
Strike Vatet Loader_eb885e48	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is eb885e485049ee4516bbdf6d9c5f202d.
Strike Vatet Loader_fc2fefb9	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is fc2fefb951bfbfdb1e337c9019968c8d.

<b>Name</b>	<b>Description</b>
Strike Vatet Loader_fe180737	This strike sends a malware sample known as Vatet Loader. Vatet is a loader that executes XOR encoded shellcode from the local disk or a network share. These loaders are often modified in order to execute the attacker's shellcode, which is usually Cobalt Strike beacons and/or stagers or as of lately the PyXie RAT payload. Vatet loader is often seen as the first stage in an Enterprise wide ransomware attack. The MD5 hash of this Vatet Loader sample is fe180737bfb5436a592581de52ed9368.
Strike VenomRAT_028b6553	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is 028b6553fc66bc01936fe9339139ecaf.
Strike VenomRAT_25b6389b	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is 25b6389bbaa746df85d53714d4a6d477.
Strike VenomRAT_25bbab0b	This strike sends a polymorphic malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this VenomRAT sample is 25bbab0b599fa4dcf98cb4f08577d9a6.
Strike VenomRAT_37fa2e7e	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is 37fa2e7e97bb22ad70d55986d1a379de.
Strike VenomRAT_38312527	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is 38312527c8f936445c85e7ddde36f420.
Strike VenomRAT_3c78cef4	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is 3c78cef4203a47012167be0877274540.

<b>Name</b>	<b>Description</b>
Strike VenomRAT_3ccc5825	This strike sends a polymorphic malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The binary has random bytes appended at the end of the file. The MD5 hash of this VenomRAT sample is 3ccc5825989d39d240d6e5e5cf296ca6.
Strike VenomRAT_406fcec2	This strike sends a polymorphic malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The binary has random bytes appended at the end of the file. The MD5 hash of this VenomRAT sample is 406fcec22aa3fd15b761f2da6cce7bc1.
Strike VenomRAT_420113e4	This strike sends a polymorphic malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this VenomRAT sample is 420113e45c86e4b023b44551ef515649.
Strike VenomRAT_46fd2b3f	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is 46fd2b3f3a94dedf52571b13875e968f.
Strike VenomRAT_571916d0	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is 571916d081469695dc35e6ee2a557827.
Strike VenomRAT_57935225	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is 57935225dcb95b6ed9894d5d5e8b46a8.

<b>Name</b>	<b>Description</b>
Strike VenomRAT_590bc27b	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is 590bc27b1f9787ebaaf5768a2eab6df.
Strike VenomRAT_5bdd41b8	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is 5bdd41b87a73c54fee015f3f42f990dd.
Strike VenomRAT_70087277	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is 70087277fa67c53783f5cbe4022bd2d1.
Strike VenomRAT_74bae7aa	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is 74bae7aac1e952c4aacda6e5861bdea5.
Strike VenomRAT_96c96ed9	This strike sends a polymorphic malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this VenomRAT sample is 96c96ed976df207337f1af1b21ffcfbb.
Strike VenomRAT_9fb172f0	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is 9fb172f0a616bf4786fab3ef452ccc0c.
Strike VenomRAT_a042db80	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is a042db8045036de713193f079fe61d6f.

<b>Name</b>	<b>Description</b>
Strike VenomRAT_a95b7d1e	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is a95b7d1ef3c4f8932fa97c287dd54c70.
Strike VenomRAT_bccaafl1e	This strike sends a polymorphic malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The binary has the timestamp field updated in the PE file header. The MD5 hash of this VenomRAT sample is bccaafl1e70e30b97e86b6c7e45c72a2f.
Strike VenomRAT_c43fffe8	This strike sends a polymorphic malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The binary has the timestamp field updated in the PE file header. The MD5 hash of this VenomRAT sample is c43fffe8372b5d06b2cc13ae7f711726.
Strike VenomRAT_c9a8aba8	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is c9a8aba8bff683df8818cf340e6c882.
Strike VenomRAT_e26ca3f0	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is e26ca3f0e251a42d708b468f79f810a9.
Strike VenomRAT_e34b6864	This strike sends a polymorphic malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this VenomRAT sample is e34b6864f95f5a3a9ed3be1cbd9e3ade.

<b>Name</b>	<b>Description</b>
Strike VenomRAT_e494fc16	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is e494fc161f1189138d1ab2a706b39303.
Strike VenomRAT_f5791878	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is f57918785e7cd4f430555e6efb00ff0f.
Strike VenomRAT_fed81eee	This strike sends a malware sample known as VenomRAT. VenomRAT is a deceptive malware delivered through a disguised shortcut file named Survey.docx.lnk. The malware poses as a legitimate Word document and deploys deceptive tactics by leveraging a genuine text file. Once executed, VenomRAT engages in keylogging, PC information leaks, and obeys commands from threat actors. The MD5 hash of this VenomRAT sample is fed81eeef57157d3ed1f399f90d2ce9a.
Strike Vobus_0a00f0e8	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 0a00f0e81031533eaf966a4e5b08dd37.
Strike Vobus_0dae873b	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 0dae873bd5aef7b73d38715011764b0f.
Strike Vobus_0e020d89	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 0e020d896441aa63ec4c0635b5918b60.
Strike Vobus_1081ceac	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 1081ceac3455fafd46c826059b13af05.
Strike Vobus_10f9ef51	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 10f9ef51258eabf3f4588e46d57ab0c0.
Strike Vobus_12c7f68a	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 12c7f68a62a8f8f86e9881959ac5e4f4.

<b>Name</b>	<b>Description</b>
Strike Vobus_13fa2468	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 13fa2468f52199836887b357ed2fb135.
Strike Vobus_150d4fd2	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 150d4fd25367f84021dcfdbaa33a8ef81.
Strike Vobus_16e1ca0f	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 16e1ca0ff1185451da68b11711ed7596.
Strike Vobus_177c4575	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 177c457533581c029508d0ed4c874d42.
Strike Vobus_183964e7	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 183964e7ec2ff6ea1fc402a6e189612a.
Strike Vobus_1df863e0	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 1df863e0fd01b6f7857bbd4378b0717d.
Strike Vobus_1e525aac	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 1e525aac0d9d1481bc49e5d19cab32f6.
Strike Vobus_28fdfdf77	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 28fdfdf7770fadf10c1ce9f18fbe59b30.
Strike Vobus_3032ff64	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 3032ff64a6e54a9bba457ae27a5c706e.
Strike Vobus_31451f44	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 31451f440278628d26cb6bbd138fd8c9.

<b>Name</b>	<b>Description</b>
Strike Vobus_31ed88b5	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 31ed88b5c4c0ab894b01da6c12f5d3b2.
Strike Vobus_3445bdee	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Vobus sample is 3445bdee16b19f4374ba974b59959a48.
Strike Vobus_3767bdf8	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 3767bdf861b334edd4d67934f3123d5b.
Strike Vobus_37fdc1d6	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 37fdc1d68ff770bdf1f464c431728f07.
Strike Vobus_380de507	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 380de50708a680b057116540ccd7a6ba.
Strike Vobus_389807c7	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 389807c710e47667a03d424b55a93431.
Strike Vobus_399163e8	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 399163e872a5b23790a334cecaa8b7b2.
Strike Vobus_3eded6b7	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 3eded6b71a9e8790f6db3845ebc4f8cd.
Strike Vobus_3f59ebdf	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 3f59ebdff512dbaec5f04844b2fc7d99.
Strike Vobus_3fe5c2a3	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 3fe5c2a38779bb813d4608b61bfaf65b.

<b>Name</b>	<b>Description</b>
Strike Vobus_438e4b20	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 438e4b2050353353b36faa4adb1c2f50.
Strike Vobus_441e0780	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 441e078085e97794e2e34b4fde44b528.
Strike Vobus_4ad43597	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 4ad43597e3f8a3442c55f1d3841e3b06.
Strike Vobus_4ad62a82	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 4ad62a8268d2128b8feac07dcd17f77d.
Strike Vobus_4c07a852	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 4c07a852f51d68fc1f795d79ff1de3c6.
Strike Vobus_4df966b7	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 4df966b7697309348dd06aba757e45c5.
Strike Vobus_542b274d	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 542b274d0fc18b0b522976e8d76f4ed2.
Strike Vobus_55c9078f	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 55c9078fdbbe765e1cd9474597c69053.
Strike Vobus_5761439a	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 5761439abee0c77d907849fe1adc111c.
Strike Vobus_57a9592b	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 57a9592ba62a296ae1baea2b2e8b9e1b.

<b>Name</b>	<b>Description</b>
Strike Vobus_58821691	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 58821691e25b385a886d2c4406545cde.
Strike Vobus_5f9bdec6	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 5f9bdec614ecd7382fd3d364e3de2e45.
Strike Vobus_636f97c9	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 636f97c9f831b9cd3c7152a65fb87c7a.
Strike Vobus_63feb8b0	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 63feb8b0f518e9e29c4ce8b23502c990.
Strike Vobus_65088181	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 650881814b785a2b2b19f1213b192a03.
Strike Vobus_659a6e89	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 659a6e8911679e7d9d9f950868452b94.
Strike Vobus_68420fb2	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 68420fb217533886291dd7d7d4dcdb4e.
Strike Vobus_69d5cef0	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 69d5cef031afef3c621594ae9fd523bf.
Strike Vobus_6b309d23	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 6b309d235c78f6ad62e77d694ec5b233.
Strike Vobus_6e07bb31	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 6e07bb31fe5a62e7cc0166de949d519b.

<b>Name</b>	<b>Description</b>
Strike Vobus_6f834648	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 6f8346481a6a4b1ba2e37e0e07ee0d42.
Strike Vobus_707da51c	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 707da51ce02acf84c26e8765f48e2ba1.
Strike Vobus_739981f3	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 739981f3099202ebdb408050ce582c3c.
Strike Vobus_73fc4025	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 73fc4025864030096c736129a6a01f94.
Strike Vobus_7872bc63	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 7872bc63d3e9dd593ae277d94f1a786f.
Strike Vobus_7d344b38	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 7d344b3816a6064e63e2cb0f49d8a539.
Strike Vobus_7f28910e	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 7f28910eca692fda8992f5cd53eaa597.
Strike Vobus_802f2a3e	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 802f2a3e702abbd0094953ada52effe5.
Strike Vobus_831c5aa7	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 831c5aa78cd391e2f37d5b60f3326dc3.
Strike Vobus_88af0388	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 88af03883badfcfb0d6f74fef2239d6c.

<b>Name</b>	<b>Description</b>
Strike Vobus_88eb5b79	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 88eb5b79c13cce02c24a27d8fd331e6a.
Strike Vobus_8bab3306	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 8bab33064756e72821c5ecff55414af3.
Strike Vobus_8d274c5b	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 8d274c5b317ad208c6ed5b6582e08f2e.
Strike Vobus_8e768ff1	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 8e768ff11aedbb72c7a6ba1767b03b25.
Strike Vobus_9110346e	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 9110346e27883b9332cd541716eb9319.
Strike Vobus_928e6edf	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 928e6edf5cb16fe36ce847cb8bc017da.
Strike Vobus_9331dc0b	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 9331dc0b87d980f61ba5d1763c16ff23.
Strike Vobus_957f96ba	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 957f96bac2a1099eea627508df4ed922.
Strike Vobus_95aa0ce2	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 95aa0ce2e3b2a6c9903431604133db2e.
Strike Vobus_97ceaaf0	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 97ceaaf009ef6ff5bec8fe75b9b7a59d.

<b>Name</b>	<b>Description</b>
Strike Vobus_98c0310d	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 98c0310d2c571aafaa12d30e2f90e764.
Strike Vobus_9bfb3525	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 9bfb352569692b9b1fcb6a4301be9441.
Strike Vobus_9c0cf03	This strike sends a polymorphic malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The binary has random bytes appended at the end of the file. The MD5 hash of this Vobus sample is 9c0cf03f3715486a737d01d0bee3b1c.
Strike Vobus_9d63fd73	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is 9d63fd73e3b8609696f382d73a02aca8.
Strike Vobus_a1bf202d	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is a1bf202de8719f61f92e2a04a4b045bf.
Strike Vobus_a2666a26	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is a2666a2695f0338c4dff0418f12dfe3.
Strike Vobus_a3c5e535	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is a3c5e5357a2736992b0b57e7d68dc38d.
Strike Vobus_a5fec6fe	This strike sends a polymorphic malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Vobus sample is a5fec6fe5d5f0733a331ad341036090d.
Strike Vobus_a76bbe69	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is a76bbe6948c53485bbf4873b44b02d40.
Strike Vobus_a786824c	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is a786824cea993c49004850e01899fe8b.

<b>Name</b>	<b>Description</b>
Strike Vobus_a9be2b20	This strike sends a polymorphic malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Vobus sample is a9be2b203cdb02bfe81a0ad9ec77dae2.
Strike Vobus_ab7c0cec	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is ab7c0cec2eca695182df07baaf1cf70d.
Strike Vobus_acae8711	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is acae8711c47ed2b31478042dd0f2072d.
Strike Vobus_ae95e19a	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is ae95e19a46c995ad8751c7480c209f0f.
Strike Vobus_b4976cd1	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is b4976cd1b26d49ccf7d42360500d06d4.
Strike Vobus_b4ed4af2	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is b4ed4af2c5cedce3f0a816f09eca7ef5.
Strike Vobus_b6b13cc1	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is b6b13cc11598445d4517172dee8f3c05.
Strike Vobus_b6b987ad	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is b6b987ad93e31f07759e37929948d190.
Strike Vobus_b6f76628	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is b6f7662876d3e2addfb387d215a0d53d.
Strike Vobus_b7a98b59	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is b7a98b59405a6badd6ce6a7f2af84a96.

<b>Name</b>	<b>Description</b>
Strike Vobus_b7ade725	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is b7ade725eefc6b098b960d75df9c5094.
Strike Vobus_b80e3b5c	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is b80e3b5c06340670203bf163dec3a646.
Strike Vobus_bbad3b46	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is bbad3b463c88c095f1cbbc2dfc9835aa.
Strike Vobus_bf6e1980	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is bf6e198066bcfdfe17ad2486b3541b27.
Strike Vobus_c2d0a004	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is c2d0a004e409f5bb3d42695e4948ac9b.
Strike Vobus_cf9ff326	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is cf9ff326fb156d353b4c44999552d7c0.
Strike Vobus_d411faa0	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is d411faa0cc22c6de3eeb58d4743b8488.
Strike Vobus_d75e1906	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is d75e1906de1f4710d0020b75d72899d2.
Strike Vobus_db14975a	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is db14975a39e6a3111bdcaf3933e97a97.
Strike Vobus_dd04f425	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is dd04f42561202ae47d160b63afbcd5e7.

<b>Name</b>	<b>Description</b>
Strike Vobus_dd36ff19	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is dd36ff19c82aa9f52d8da1ce2490f6f9.
Strike Vobus_df7e2da9	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is df7e2da992ca71bcdab446c0e8ea3ba0.
Strike Vobus_e00e4957	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is e00e49576a444ca240298abe1d3e4b7f.
Strike Vobus_e1139afb	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is e1139afbb90c870ad7972db462abd0b4.
Strike Vobus_e36daaa1	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is e36daaa1ebc06af7c2ddb48e610678a0.
Strike Vobus_e53b3e8d	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is e53b3e8d99502c685f210423ce531916.
Strike Vobus_e7168104	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is e716810407e2023354e61ee5f1346070.
Strike Vobus_e7f6b759	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is e7f6b7599c9f3fe7d4958212b1c7ff12.
Strike Vobus_ecf3ac1c	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is ecf3ac1cee6d87326ad9642c16114e30.
Strike Vobus_ed7bf69c	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is ed7bf69c51703dc87080a21b175f0f77.

<b>Name</b>	<b>Description</b>
Strike Vobus_f1a80e8e	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is f1a80e8e0bf490bef55703eaf022ad86.
Strike Vobus_f4408023	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is f4408023aeb40b2e238f3b4d74d00ec5.
Strike Vobus_f5ba3f0a	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is f5ba3f0ac575d509f55461b1766a1494.
Strike Vobus_f74bb0ef	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is f74bb0efe406b6b15c475ecab70a15f7.
Strike Vobus_f9ccc250	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is f9ccc2505a03bcaa4ca3b7016a126d7a.
Strike Vobus_fd366286	This strike sends a polymorphic malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Vobus sample is fd36628620e5824ff4179536c9a12a77.
Strike Vobus_fe04e2e4	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is fe04e2e401407bc1c641d8218ef88580.
Strike Vobus_fed72db4	This strike sends a malware sample known as Vobus. Vobus is a worm that spreads itself through removable drives. After the malware executes it often downloads follow on malware payloads for additional task. The MD5 hash of this Vobus sample is fed72db48b981763a8846d98146a909d.
Strike Volt Typhoon_2b698923	This strike sends a malware sample known as Volt Typhoon. Volt Typhoon is a Chinese state sponsored group that delivers campaigns against targets with a focus on espionage and information gathering. The malware in their campaign requires command line commands, and tailored attacks on their target including credential theft from local and network systems to allow for persistence. They also include custom FRP executables that allow them to communicate with a C2 channel over a proxy. This malware is one of the custom FRP executables. The MD5 hash of this Volt Typhoon sample is 2b6989231cdae585e66994268b15d609.

<b>Name</b>	<b>Description</b>
Strike Volt Typhoon_308cd259	This strike sends a malware sample known as Volt Typhoon. Volt Typhoon is a Chinese state sponsored group that delivers campaigns against targets with a focus on espionage and information gathering. The malware in their campaign requires command line commands, and tailored attacks on their target including credential theft from local and network systems to allow for persistence. They also include custom FRP executables that allow them to communicate with a C2 channel over a proxy. This malware is one of the custom FRP executables. The MD5 hash of this Volt Typhoon sample is 308cd259bb9b0ed17c876881852e7992.
Strike Volt Typhoon_433331fe	This strike sends a malware sample known as Volt Typhoon. Volt Typhoon is a Chinese state sponsored group that delivers campaigns against targets with a focus on espionage and information gathering. The malware in their campaign requires command line commands, and tailored attacks on their target including credential theft from local and network systems to allow for persistence. They also include custom FRP executables that allow them to communicate with a C2 channel over a proxy. This malware is one of the custom FRP executables. The MD5 hash of this Volt Typhoon sample is 433331fe1a3ff11ea362fc772b67da38.
Strike Volt Typhoon_640527a0	This strike sends a malware sample known as Volt Typhoon. Volt Typhoon is a Chinese state sponsored group that delivers campaigns against targets with a focus on espionage and information gathering. The malware in their campaign requires command line commands, and tailored attacks on their target including credential theft from local and network systems to allow for persistence. They also include custom FRP executables that allow them to communicate with a C2 channel over a proxy. This malware is one of the custom FRP executables. The MD5 hash of this Volt Typhoon sample is 640527a052a0fa57c58dd1a4a4628ec2.
Strike Volt Typhoon_80d52999	This strike sends a malware sample known as Volt Typhoon. Volt Typhoon is a Chinese state sponsored group that delivers campaigns against targets with a focus on espionage and information gathering. The malware in their campaign requires command line commands, and tailored attacks on their target including credential theft from local and network systems to allow for persistence. They also include custom FRP executables that allow them to communicate with a C2 channel over a proxy. This malware is one of the custom FRP executables. The MD5 hash of this Volt Typhoon sample is 80d52999032325876d68cda01eb634db.
Strike Volt Typhoon_989c12b2	This strike sends a malware sample known as Volt Typhoon. Volt Typhoon is a Chinese state sponsored group that delivers campaigns against targets with a focus on espionage and information gathering. The malware in their campaign requires command line commands, and tailored attacks on their target including credential theft from local and network systems to allow for persistence. They also include custom FRP executables that allow them to communicate with a C2 channel over a proxy. This malware is one of the custom FRP executables. The MD5 hash of this Volt Typhoon sample is 989c12b22ae56d5bc6249047119a9ed1.

<b>Name</b>	<b>Description</b>
Strike Volt Typhoon_a0254a82	This strike sends a malware sample known as Volt Typhoon. Volt Typhoon is a Chinese state sponsored group that delivers campaigns against targets with a focus on espionage and information gathering. The malware in their campaign requires command line commands, and tailored attacks on their target including credential theft from local and network systems to allow for persistence. They also include custom FRP executables that allow them to communicate with a C2 channel over a proxy. This malware is one of the custom FRP executables. The MD5 hash of this Volt Typhoon sample is a0254a824d9adcd2f173923acfe4da7f.
Strike Volt Typhoon_c6d185d2	This strike sends a malware sample known as Volt Typhoon. Volt Typhoon is a Chinese state sponsored group that delivers campaigns against targets with a focus on espionage and information gathering. The malware in their campaign requires command line commands, and tailored attacks on their target including credential theft from local and network systems to allow for persistence. They also include custom FRP executables that allow them to communicate with a C2 channel over a proxy. This malware is one of the custom FRP executables. The MD5 hash of this Volt Typhoon sample is c6d185d2c1dbfc3a5073e0dc580e8.
Strike Volt Typhoon_d241145b	This strike sends a malware sample known as Volt Typhoon. Volt Typhoon is a Chinese state sponsored group that delivers campaigns against targets with a focus on espionage and information gathering. The malware in their campaign requires command line commands, and tailored attacks on their target including credential theft from local and network systems to allow for persistence. They also include custom FRP executables that allow them to communicate with a C2 channel over a proxy. This malware is one of the custom FRP executables. The MD5 hash of this Volt Typhoon sample is d241145b848ce17c6a547c411ff9eff8.
Strike Volt Typhoon_d35cb972	This strike sends a malware sample known as Volt Typhoon. Volt Typhoon is a Chinese state sponsored group that delivers campaigns against targets with a focus on espionage and information gathering. The malware in their campaign requires command line commands, and tailored attacks on their target including credential theft from local and network systems to allow for persistence. They also include custom FRP executables that allow them to communicate with a C2 channel over a proxy. This malware is one of the custom FRP executables. The MD5 hash of this Volt Typhoon sample is d35cb972271a75cdc3a9900ed7f40a37.
Strike Volt Typhoon_e6456b4c	This strike sends a malware sample known as Volt Typhoon. Volt Typhoon is a Chinese state sponsored group that delivers campaigns against targets with a focus on espionage and information gathering. The malware in their campaign requires command line commands, and tailored attacks on their target including credential theft from local and network systems to allow for persistence. They also include custom FRP executables that allow them to communicate with a C2 channel over a proxy. This malware is one of the custom FRP executables. The MD5 hash of this Volt Typhoon sample is e6456b4c14be0921616b28c219386e1a.
Strike Vultur_0de7a913	This strike sends a malware sample known as Vultur. Vultur is an Android banking malware that targets a mobile device running the Android operating system. It contains many features like keylogging, screen recording, and remote control capabilities. Recently it has been associated with the Brunhilda dropper-framework which was deployed via SMS messages. The MD5 hash of this Vultur sample is 0de7a9134f17bacb35e6bc712bdc6923.

<b>Name</b>	<b>Description</b>
Strike Vultur_127ac542	This strike sends a polymorphic malware sample known as Vultur. Vultur is an Android banking malware known for its screen recording and remote control functionalities. It spreads through a hybrid attack leveraging SMS and phone calls to trick victims into installing trojanized applications, masquerading as the Brunhilda dropper. Some key features of Vultur include its ability to remotely interact with infected devices using Android's Accessibility Services, along with features like app blocking, custom notifications, and evasion of lock screen security measures. The malware employs sophisticated anti-analysis tactics, such as AES encryption and Base64 encoding for C2 communication. 'com.medical.balance' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 127ac54287280f06ce621f1ba0a12218.
Strike Vultur_2e5373ac	This strike sends a polymorphic malware sample known as Vultur. Vultur is an Android banking malware known for its screen recording and remote control functionalities. It spreads through a hybrid attack leveraging SMS and phone calls to trick victims into installing trojanized applications, masquerading as the Brunhilda dropper. Some key features of Vultur include its ability to remotely interact with infected devices using Android's Accessibility Services, along with features like app blocking, custom notifications, and evasion of lock screen security measures. The malware employs sophisticated anti-analysis tactics, such as AES encryption and Base64 encoding for C2 communication. 'com.medical.balance' is the package name of the malware sample. Constant strings in the code has been encrypted. The MD5 hash of this malware sample is 2e5373ac241477077ffa04b948859348.
Strike Vultur_753bf0cd	This strike sends a polymorphic malware sample known as Vultur. Vultur is an Android banking malware known for its screen recording and remote control functionalities. It spreads through a hybrid attack leveraging SMS and phone calls to trick victims into installing trojanized applications, masquerading as the Brunhilda dropper. Some key features of Vultur include its ability to remotely interact with infected devices using Android's Accessibility Services, along with features like app blocking, custom notifications, and evasion of lock screen security measures. The malware employs sophisticated anti-analysis tactics, such as AES encryption and Base64 encoding for C2 communication. 'com.medical.balance' is the package name of the malware sample. The malware has been rebuilt without any mofifications. The MD5 hash of this malware sample is 753bf0cd0e154893f8bd36c12740a7ed.
Strike Vultur_8bc072db	This strike sends a malware sample known as Vultur. Vultur is an Android banking malware that targets a mobile device running the Android operating system. It contains many features like keylogging, screen recording, and remote control capabilities. Recently it has been associated with the Brunhilda dropper-framework which was deployed via SMS messages. The MD5 hash of this Vultur sample is 8bc072db670a9a92860ad0cfb404d3a8.
Strike Vultur_8e83d178	This strike sends a malware sample known as Vultur. Vultur is an Android banking malware that targets a mobile device running the Android operating system. It contains many features like keylogging, screen recording, and remote control capabilities. Recently it has been associated with the Brunhilda dropper-framework which was deployed via SMS messages. The MD5 hash of this Vultur sample is 8e83d178c1a3b9da0c71c613e2c77647.

<b>Name</b>	<b>Description</b>
Strike Vultur_979bd87a	This strike sends a polymorphic malware sample known as Vultur. Vultur is an Android banking malware known for its screen recording and remote control functionalities. It spreads through a hybrid attack leveraging SMS and phone calls to trick victims into installing trojanized applications, masquerading as the Brunhilda dropper. Some key features of Vultur include its ability to remotely interact with infected devices using Android's Accessibility Services, along with features like app blocking, custom notifications, and evasion of lock screen security measures. The malware employs sophisticated anti-analysis tactics, such as AES encryption and Base64 encoding for C2 communication. 'com.medical.balance' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 979bd87a975a128fe51cd46eaeaf2123.
Strike Vultur_a02059f5	This strike sends a polymorphic malware sample known as Vultur. Vultur is an Android banking malware known for its screen recording and remote control functionalities. It spreads through a hybrid attack leveraging SMS and phone calls to trick victims into installing trojanized applications, masquerading as the Brunhilda dropper. Some key features of Vultur include its ability to remotely interact with infected devices using Android's Accessibility Services, along with features like app blocking, custom notifications, and evasion of lock screen security measures. The malware employs sophisticated anti-analysis tactics, such as AES encryption and Base64 encoding for C2 communication. 'com.medical.balance' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is a02059f5f198a55d8a20d452ae6f0c05.
Strike Vultur_b338d679	This strike sends a malware sample known as Vultur. Vultur is an Android banking malware that targets a mobile device running the Android operating system. It contains many features like keylogging, screen recording, and remote control capabilities. Recently it has been associated with the Brunhilda dropper-framework which was deployed via SMS messages. The MD5 hash of this Vultur sample is b338d679ba2ad31515fac6098c4fd9a3.
Strike Vultur_b58a7cc0	This strike sends a malware sample known as Vultur. Vultur is an Android banking malware that targets a mobile device running the Android operating system. It contains many features like keylogging, screen recording, and remote control capabilities. Recently it has been associated with the Brunhilda dropper-framework which was deployed via SMS messages. The MD5 hash of this Vultur sample is b58a7cc0c8cf529ae05589f8b76cd8a7.
Strike Vultur_b6366aa9	This strike sends a malware sample known as Vultur. Vultur is an Android banking malware known for its screen recording and remote control functionalities. It spreads through a hybrid attack leveraging SMS and phone calls to trick victims into installing trojanized applications, masquerading as the Brunhilda dropper. Some key features of Vultur include its ability to remotely interact with infected devices using Android's Accessibility Services, along with features like app blocking, custom notifications, and evasion of lock screen security measures. The malware employs sophisticated anti-analysis tactics, such as AES encryption and Base64 encoding for C2 communication. 'com.medical.balance' is the package name of the malware sample. The MD5 hash of this malware sample is b6366aa97dde56a0aa4f3f307111107f.

<b>Name</b>	<b>Description</b>
Strike Vultur_c9f6942b	This strike sends a malware sample known as Vultur. Vultur is an Android banking malware that targets a mobile device running the Android operating system. It contains many features like keylogging, screen recording, and remote control capabilities. Recently it has been associated with the Brunhilda dropper-framework which was deployed via SMS messages. The MD5 hash of this Vultur sample is c9f6942b74e70d06726542cbcce989f7.
Strike Vultur_d80c9982	This strike sends a malware sample known as Vultur. Vultur is an Android banking malware known for its screen recording and remote control functionalities. It spreads through a hybrid attack leveraging SMS and phone calls to trick victims into installing trojanized applications, masquerading as the Brunhilda dropper. Some key features of Vultur include its ability to remotely interact with infected devices using Android's Accessibility Services, along with features like app blocking, custom notifications, and evasion of lock screen security measures. The malware employs sophisticated anti-analysis tactics, such as AES encryption and Base64 encoding for C2 communication. 'com.medical.balance' is the package name of the malware sample. The MD5 hash of this malware sample is d80c998228046321e2a19e19968af3c6.
Strike Vultur_faea40b1	This strike sends a polymorphic malware sample known as Vultur. Vultur is an Android banking malware known for its screen recording and remote control functionalities. It spreads through a hybrid attack leveraging SMS and phone calls to trick victims into installing trojanized applications, masquerading as the Brunhilda dropper. Some key features of Vultur include its ability to remotely interact with infected devices using Android's Accessibility Services, along with features like app blocking, custom notifications, and evasion of lock screen security measures. The malware employs sophisticated anti-analysis tactics, such as AES encryption and Base64 encoding for C2 communication. 'com.medical.balance' is the package name of the malware sample. Constant strings in the code has been encrypted. The MD5 hash of this malware sample is faea40b1c43d87beabe2616736e8dd58.
Strike Weaver Ant_3f46a223	This strike sends a malware sample known as Weaver Ant. Weaver Ant is the name of a China-nexus threat group associated with an attack against a major Asian telecommunication company. This attack employed variants of the China Chopper web shell and this sample was detected in the attack. The MD5 hash of this Weaver Ant sample is 3f46a22398fffa3e43caff35034a6bae.
Strike Weaver Ant_49295998	This strike sends a malware sample known as Weaver Ant. Weaver Ant is the name of a China-nexus threat group associated with an attack against a major Asian telecommunication company. This attack employed variants of the China Chopper web shell and this sample was detected in the attack. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Weaver Ant sample is 49295998ca3dbba3179a083d15c5ac3f.
Strike Whiffy Recon_00923097	This strike sends a malware sample known as Whiffy Recon. Whiffy Recon is malware that has been detected being delivered via the Smoke Loader botnet. The malware looks for the WLANSVC service on a system and will exit if it does not exist. This malware scans for wifi access points using the Windows WLAN API, and sends POST requests to Google's Geolocation API. This provides the coordinates to the location of the access points which gets sent recorded and sent back to the attacker C2 server via an authorization UUID. The MD5 hash of this Whiffy Recon sample is 009230972491f5f5079e8e86e19d5458.

Name	Description
Strike Whiffy Recon_649b89c4	This strike sends a polymorphic malware sample known as Whiffy Recon. Whiffy Recon is malware that has been detected being delivered via the Smoke Loader botnet. The malware looks for the WLANSVC service on a system and will exit if it does not exist. This malware scans for wifi access points using the Windows WLAN API, and sends POST requests to Google's Geolocation API. This provides the coordinates to the location of the access points which gets sent recorded and sent back to the attacker C2 server via an authorization UUID. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Whiffy Recon sample is 649b89c4e9e8e7063966ee87350398b9.
Strike Whiffy Recon_801b4814	This strike sends a polymorphic malware sample known as Whiffy Recon. Whiffy Recon is malware that has been detected being delivered via the Smoke Loader botnet. The malware looks for the WLANSVC service on a system and will exit if it does not exist. This malware scans for wifi access points using the Windows WLAN API, and sends POST requests to Google's Geolocation API. This provides the coordinates to the location of the access points which gets sent recorded and sent back to the attacker C2 server via an authorization UUID. The binary has the debug flag removed in the PE file format. The MD5 hash of this Whiffy Recon sample is 801b4814ad8066e447d65fcfd641aa70.
Strike Whiffy Recon_bc2dfa0b	This strike sends a polymorphic malware sample known as Whiffy Recon. Whiffy Recon is malware that has been detected being delivered via the Smoke Loader botnet. The malware looks for the WLANSVC service on a system and will exit if it does not exist. This malware scans for wifi access points using the Windows WLAN API, and sends POST requests to Google's Geolocation API. This provides the coordinates to the location of the access points which gets sent recorded and sent back to the attacker C2 server via an authorization UUID. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Whiffy Recon sample is bc2dfa0b70de83c33e7d586144860f60.
Strike Whiffy Recon_d19b1629	This strike sends a polymorphic malware sample known as Whiffy Recon. Whiffy Recon is malware that has been detected being delivered via the Smoke Loader botnet. The malware looks for the WLANSVC service on a system and will exit if it does not exist. This malware scans for wifi access points using the Windows WLAN API, and sends POST requests to Google's Geolocation API. This provides the coordinates to the location of the access points which gets sent recorded and sent back to the attacker C2 server via an authorization UUID. The binary has been packed using upx packer, with the default options. The MD5 hash of this Whiffy Recon sample is d19b16297b2bd695850a4131cd08bca9.
Strike Whiffy Recon_e33265c3	This strike sends a polymorphic malware sample known as Whiffy Recon. Whiffy Recon is malware that has been detected being delivered via the Smoke Loader botnet. The malware looks for the WLANSVC service on a system and will exit if it does not exist. This malware scans for wifi access points using the Windows WLAN API, and sends POST requests to Google's Geolocation API. This provides the coordinates to the location of the access points which gets sent recorded and sent back to the attacker C2 server via an authorization UUID. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Whiffy Recon sample is e33265c35509acd382779fca4103bdf2.

<b>Name</b>	<b>Description</b>
Strike WhisperGate DLL Loader_b3370eb3	This strike sends a malware sample known as WhisperGate DLL Loader. In January 2022 the WhisperGate malware was detected in cyber attacks being conducted against the Ukrainian Government. WhisperGate is a multi-stage malware that masquerades as ransomware. It downloads a payload that wipes the MBR, then downloads a malicious file from a Discord server. This last file drops and executes a final wiper payload that enumerates the drives on the system and proceeds to wipe all files with specific extensions. This sample is the DLL Loader. The MD5 hash of this WhisperGate DLL Loader sample is b3370eb3c5ef6c536195b3bea0120929.
Strike WhisperGate DLL Loader_e61518ae	This strike sends a malware sample known as WhisperGate DLL Loader. In January 2022 the WhisperGate malware was detected in cyber attacks being conducted against the Ukrainian Government. WhisperGate is a multi-stage malware that masquerades as ransomware. It downloads a payload that wipes the MBR, then downloads a malicious file from a Discord server. This last file drops and executes a final wiper payload that enumerates the drives on the system and proceeds to wipe all files with specific extensions. This sample is the DLL Loader. The MD5 hash of this WhisperGate DLL Loader sample is e61518ae9454a563b8f842286bbdb87b.
Strike WhisperGate Downloader_14c8482f	This strike sends a malware sample known as WhisperGate Downloader. In January 2022 the WhisperGate malware was detected in cyber attacks being conducted against the Ukrainian Government. WhisperGate is a multi-stage malware that masquerades as ransomware. It downloads a payload that wipes the MBR, then downloads a malicious file from a Discord server. This last file drops and executes a final wiper payload that enumerates the drives on the system and proceeds to wipe all files with specific extensions. This sample is the Downloader. The MD5 hash of this WhisperGate Downloader sample is 14c8482f302b5e81e3fa1b18a509289d.
Strike WhisperGate Downloader_87037d61	This strike sends a polymorphic malware sample known as WhisperGate Downloader. In January 2022 the WhisperGate malware was detected in cyber attacks being conducted against the Ukrainian Government. WhisperGate is a multi-stage malware that masquerades as ransomware. It downloads a payload that wipes the MBR, then downloads a malicious file from a Discord server. This last file drops and executes a final wiper payload that enumerates the drives on the system and proceeds to wipe all files with specific extensions. This sample is the Downloader. The binary has the timestamp field updated in the PE file header. The MD5 hash of this WhisperGate Downloader sample is 87037d614242a155e033dcf1a4e23edc.
Strike WhisperGate Downloader_ba93cdc0	This strike sends a polymorphic malware sample known as WhisperGate Downloader. In January 2022 the WhisperGate malware was detected in cyber attacks being conducted against the Ukrainian Government. WhisperGate is a multi-stage malware that masquerades as ransomware. It downloads a payload that wipes the MBR, then downloads a malicious file from a Discord server. This last file drops and executes a final wiper payload that enumerates the drives on the system and proceeds to wipe all files with specific extensions. This sample is the Downloader. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this WhisperGate Downloader sample is ba93cdc021c860abd7015f933b4b795e.

<b>Name</b>	<b>Description</b>
Strike WhisperGate Downloader_bfb1c1c2c2	This strike sends a polymorphic malware sample known as WhisperGate Downloader. In January 2022 the WhisperGate malware was detected in cyber attacks being conducted against the Ukrainian Government. WhisperGate is a multi-stage malware that masquerades as ransomware. It downloads a payload that wipes the MBR, then downloads a malicious file from a Discord server. This last file drops and executes a final wiper payload that enumerates the drives on the system and proceeds to wipe all files with specific extensions. This sample is the Downloader. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this WhisperGate Downloader sample is bfb1c2c2ed861fb7435533378304574.
Strike WhisperGate MBR Wiper_5d5c99a0	This strike sends a malware sample known as WhisperGate MBR Wiper. In January 2022 the WhisperGate malware was detected in cyber attacks being conducted against the Ukrainian Government. WhisperGate is a multi-stage malware that masquerades as ransomware. It downloads a payload that wipes the MBR, then downloads a malicious file from a Discord server. This last file drops and executes a final wiper payload that enumerates the drives on the system and proceeds to wipe all files with specific extensions. This sample is the MBR Wiper. The MD5 hash of this WhisperGate MBR Wiper sample is 5d5c99a08a7d927346ca2dafa7973fc1.
Strike WhisperKill Wiper_22bd9ed6	This strike sends a polymorphic malware sample known as WhisperKill Wiper. In January 2022 the WhisperGate malware was detected in cyber attacks being conducted against the Ukrainian Government. WhisperGate is a multi-stage malware that masquerades as ransomware. It downloads a payload that wipes the MBR, then downloads a malicious file from a Discord server. This last file drops and executes a final wiper payload that enumerates the drives on the system and proceeds to wipe all files with specific extensions. This sample is the final wiper. The binary has been packed using upx packer, with the default options. The MD5 hash of this WhisperKill Wiper sample is 22bd9ed61d794576b42ccc477dc53e00.
Strike WhisperKill Wiper_3907c7fb	This strike sends a malware sample known as WhisperKill Wiper. In January 2022 the WhisperGate malware was detected in cyber attacks being conducted against the Ukrainian Government. WhisperGate is a multi-stage malware that masquerades as ransomware. It downloads a payload that wipes the MBR, then downloads a malicious file from a Discord server. This last file drops and executes a final wiper payload that enumerates the drives on the system and proceeds to wipe all files with specific extensions. This sample is the final wiper. The MD5 hash of this WhisperKill Wiper sample is 3907c7fdb4148395284d8e6e3c1dba5d.
Strike WhisperKill Wiper_4b0e0fce	This strike sends a polymorphic malware sample known as WhisperKill Wiper. In January 2022 the WhisperGate malware was detected in cyber attacks being conducted against the Ukrainian Government. WhisperGate is a multi-stage malware that masquerades as ransomware. It downloads a payload that wipes the MBR, then downloads a malicious file from a Discord server. This last file drops and executes a final wiper payload that enumerates the drives on the system and proceeds to wipe all files with specific extensions. This sample is the final wiper. The binary has the checksum removed in the PE file format. The MD5 hash of this WhisperKill Wiper sample is 4b0e0fce7b043861ff2731a83a4b4df0.

<b>Name</b>	<b>Description</b>
Strike WhisperKill Wiper_724ee459	This strike sends a polymorphic malware sample known as WhisperKill Wiper. In January 2022 the WhisperGate malware was detected in cyber attacks being conducted against the Ukrainian Government. WhisperGate is a multi-stage malware that masquerades as ransomware. It downloads a payload that wipes the MBR, then downloads a malicious file from a Discord server. This last file drops and executes a final wiper payload that enumerates the drives on the system and proceeds to wipe all files with specific extensions. This sample is the final wiper. The binary has random bytes appended at the end of the file. The MD5 hash of this WhisperKill Wiper sample is 724ee45952d709be7c79d7d1f1497ea2.
Strike WhisperKill Wiper_75a007bf	This strike sends a polymorphic malware sample known as WhisperKill Wiper. In January 2022 the WhisperGate malware was detected in cyber attacks being conducted against the Ukrainian Government. WhisperGate is a multi-stage malware that masquerades as ransomware. It downloads a payload that wipes the MBR, then downloads a malicious file from a Discord server. This last file drops and executes a final wiper payload that enumerates the drives on the system and proceeds to wipe all files with specific extensions. This sample is the final wiper. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this WhisperKill Wiper sample is 75a007bf2b9b25e66bba3b10d3094511.
Strike WhisperKill Wiper_a6615ab8	This strike sends a polymorphic malware sample known as WhisperKill Wiper. In January 2022 the WhisperGate malware was detected in cyber attacks being conducted against the Ukrainian Government. WhisperGate is a multi-stage malware that masquerades as ransomware. It downloads a payload that wipes the MBR, then downloads a malicious file from a Discord server. This last file drops and executes a final wiper payload that enumerates the drives on the system and proceeds to wipe all files with specific extensions. This sample is the final wiper. The binary file has one more imports added in the import table. The MD5 hash of this WhisperKill Wiper sample is a6615ab8fb6f99fd82569cbfa5762a5f.
Strike WinorDLL64_13a44e55	This strike sends a malware sample known as WinorDLL64. The WinorDLL64 malware has recently been attributed to the Lazarus APT group. It is a recently discovered payload of the Wslink Downloader malware. The payload serves as a backdoor that acquires system information, can exfiltrate files and execute additional commands. The MD5 hash of this WinorDLL64 sample is 13a44e5599c225d88d20398b4bec842a.
Strike WyrmSpy_015f01ca	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is 015f01cacca56bb4c8b1978a29194491.

<b>Name</b>	<b>Description</b>
Strike WyrmSpy_0424b9dc	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is 0424b9dca148e291178acae85797b9e3.
Strike WyrmSpy_11c73a0c	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is 11c73a0c0239c1b4c8687f938bb62994.
Strike WyrmSpy_1f139e86	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is 1f139e861e413544b13744b9f28bc197.
Strike WyrmSpy_2750e220	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is 2750e220054bd64faabb10b50a2294bd.
Strike WyrmSpy_38fe6f99	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is 38fe6f997303b30244d41f3939b64448.

<b>Name</b>	<b>Description</b>
Strike WyrmSpy_501b612d	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is 501b612d7dac6cae533f84a8c6ac476b.
Strike WyrmSpy_650ab382	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is 650ab382058af1b5fab17e12ca7d34f9.
Strike WyrmSpy_77dcf237	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is 77dcf23759bf5ced8a0a0528e49ab413.
Strike WyrmSpy_80c86ebd	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is 80c86ebd37589d4b65ce80c2c48d0868.
Strike WyrmSpy_96af63ce	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is 96af63ce9d21a0ba8b896f05f567fc6a.

<b>Name</b>	<b>Description</b>
Strike WyrmSpy_984fd47f	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is 984fd47f5950ff4b298df323417105aa.
Strike WyrmSpy_9c1bed66	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is 9c1bed665f214e8fc77fc388baedc2a1.
Strike WyrmSpy_a0c9fbab	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is a0c9fbaba91d52de183f877e66e0f34e.
Strike WyrmSpy_aceb3bb5	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is aceb3bb56c94145aa35393d4f9bc8506.
Strike WyrmSpy_aec0f309	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is aec0f30914ffabdf797dab23c74e7c98.

<b>Name</b>	<b>Description</b>
Strike WyrmSpy_b5e44369	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is b5e44369b774205ef744cbafe86df427.
Strike WyrmSpy_c06aedd7	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is c06aedd759158d438a01117f1df7da72.
Strike WyrmSpy_c77842c3	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is c77842c3bb14316476d220685441276a.
Strike WyrmSpy_cba226f0	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is cba226f05eae72c7c8680f6ee47fd66c.
Strike WyrmSpy_cc14fa95	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is cc14fa959b6409e9ac566fb4e6ed92d7.

<b>Name</b>	<b>Description</b>
Strike WyrmSpy_d5ba859e	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is d5ba859ee3b4676415b6265a6b4fa29a.
Strike WyrmSpy_da8e17f6	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is da8e17f6380a617142636b0927abbecef.
Strike WyrmSpy_e194825f	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is e194825fe6454a69ff1d74313afd43d4.
Strike WyrmSpy_efba92e5	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is efba92e52f815a0fbe00b88a81172707.
Strike WyrmSpy_f499f7e4	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is f499f7e4fbf7909f72d87db7b429e36d.

<b>Name</b>	<b>Description</b>
Strike WyrmSpy_feea40f6	This strike sends a malware sample known as WyrmSpy. WyrmSpy is an Android surveillanceware that has been attributed to the APT41 group. This malware has data collection and exfiltration capabilities. The app masquerades as a default Android OS system app used to display notifications to the user. It has also been detected posing as adult video content, a food delivery platform, and Adobe Flash. Once the app is installed it downloads additional modules to give it further capabilities. These capabilities include escalating privileges, communicating with C2 servers to upload log files, photos, and conduct surveillance on the device to allow for exfiltration of additional data like SMS text and audio. The MD5 hash of this WyrmSpy sample is feea40f6289356e11670ccf6c80f76c6.
Strike XMRig Miner_1b43ac36	This strike sends a malware sample known as XMRig Miner. xmrig miner for campaign The MD5 hash of this XMRig Miner sample is 1b43ac369ff1d3e5564980add99d9e52.
Strike XMRig Miner_e2a07222	This strike sends a malware sample known as XMRig Miner. xmrig miner for campaign The MD5 hash of this XMRig Miner sample is e2a072228078e6f3cf5073f4af029913.
Strike XMRig Miner_e43cca48	This strike sends a malware sample known as XMRig Miner. xmrig miner for campaign The MD5 hash of this XMRig Miner sample is e43cca482b19e8c05daefb2c36a67144.
Strike XZ Backdoor_033d56fc	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 033d56fc757686037be736c89727b3f9.
Strike XZ Backdoor_079d41f2	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 079d41f2e76288f1fdd65e72bf58c304.
Strike XZ Backdoor_153df972	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 153df9727a2729879a26c1995007ffbc.
Strike XZ Backdoor_18c35cec	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 18c35cece465de482063a1fd801b1f44.

<b>Name</b>	<b>Description</b>
Strike XZ Backdoor_212ffa0b	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 212ffa0b24bb7d749532425a46764433.
Strike XZ Backdoor_24544dc0	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 24544dc0359a3ecdbea7e463f45c3c3f.
Strike XZ Backdoor_24980143	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 24980143937d9ed3f3e36852e4397f2e.
Strike XZ Backdoor_264366ac	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 264366ac4b5dfca93fabd047a938268f.
Strike XZ Backdoor_2ee85780	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 2ee857800914b90dbccf7d448f5f6339.
Strike XZ Backdoor_3178b98a	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 3178b98a7cebbb7343d16858fb4df2ff.
Strike XZ Backdoor_35028f4b	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 35028f4b5c6673d6f2e1a80f02944fb2.
Strike XZ Backdoor_3ffb426	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 3ffb426381c011dc9c986376d944ab7.

<b>Name</b>	<b>Description</b>
Strike XZ Backdoor_42812f07	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 42812f07915f216244ef1a03d2380f7d.
Strike XZ Backdoor_42a48cea	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 42a48cea544ce30b33135466cdca80d2.
Strike XZ Backdoor_4ec47410	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 4ec47410372386d02c432ba10e5d7fda.
Strike XZ Backdoor_4f0cf1d2	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 4f0cf1d2a2d44b75079b3ea5ed28fe54.
Strike XZ Backdoor_5128f091	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 5128f09111ad537617d8b6780cfbce0a.
Strike XZ Backdoor_53d82bb5	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 53d82bb511b71a5d4794cf2d8a2072c1.
Strike XZ Backdoor_540c665d	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 540c665dfcd4e5cfba5b72b4787fec4f.
Strike XZ Backdoor_5aeddab5	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 5aeddab53ee2cbd694f901a080f84bf1.

<b>Name</b>	<b>Description</b>
Strike XZ Backdoor_609fd075	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 609fd075f1a0618a54c0ebc43b4da718.
Strike XZ Backdoor_645ac58a	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 645ac58a2301ef1685f32fe30b3f01e1.
Strike XZ Backdoor_64de5a2b	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 64de5a2b7a692afa301fdbd9755ef0de0.
Strike XZ Backdoor_6efd76c6	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 6efd76c69f61a87e175c198f30b9dab8.
Strike XZ Backdoor_7aeec6f9	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 7aeec6f9431742ca3afb46b7b96678eb.
Strike XZ Backdoor_87e595fb	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 87e595fb7cf67af0d9ce331c564a6bf5.
Strike XZ Backdoor_89e11f41	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 89e11f41c5acf6c641b19230dc5cdea.
Strike XZ Backdoor_8acaf066	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 8acaf0667c311c4c44d3d1ae2855b7d4.

<b>Name</b>	<b>Description</b>
Strike XZ Backdoor_8e409b9d	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 8e409b9d6ff3a0d4998aa9d67bd13467.
Strike XZ Backdoor_906b3611	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 906b3611f5349bfb096e74188bdc8994.
Strike XZ Backdoor_957a7b21	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 957a7b218b1da7fd90c579581a8430fb.
Strike XZ Backdoor_9e2095fb	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is 9e2095fb065c9221fa8c847f783c4af3.
Strike XZ Backdoor_a15a638a	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is a15a638ac2710ca445408549ee752bf7.
Strike XZ Backdoor_a49cfa85	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is a49cfa85d7d4efab30f84a57e70d8dea.
Strike XZ Backdoor_a636cd9e	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is a636cd9e3918d1336b9a368f8125410c.
Strike XZ Backdoor_a78380f6	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is a78380f647766a2bc099844375bd5a4c.

<b>Name</b>	<b>Description</b>
Strike XZ Backdoor_ac3b4d9f	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is ac3b4d9f163c90143f938627473a804a.
Strike XZ Backdoor_b6bd548c	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is b6bd548cd38529097270ccb9059afa23.
Strike XZ Backdoor_bd98943a	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is bd98943a55ea3ca03a3af6824a42c8b1.
Strike XZ Backdoor_c2b52851	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is c2b5285108fe0bb9c585a8afd2029296.
Strike XZ Backdoor_c38d85f7	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is c38d85f769c82d82b3519db876a5fdc6.
Strike XZ Backdoor_c518d573	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is c518d573a716b2b2bc2413e6c9b5dbde.
Strike XZ Backdoor_c77fa4da	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is c77fa4dab4df4b976681571dd11bcab1.
Strike XZ Backdoor_ceb6b4bb	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is ceb6b4bbae548fd71213b6d272976ee3.

<b>Name</b>	<b>Description</b>
Strike XZ Backdoor_cfb1afdf	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is cfb1afdfcfeca02f7677b1b401bc536e.
Strike XZ Backdoor_d26cefd9	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is d26cefd934b33b174a795760fc79e6b5.
Strike XZ Backdoor_d302c6cb	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is d302c6cb2fa1c03c710fa5285651530f.
Strike XZ Backdoor_d32d7710	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is d32d7710ddca687c5d3ead014a395fd9.
Strike XZ Backdoor_edfb3661	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is edfb3661736e46ab3954bebbf7dc4b5c.
Strike XZ Backdoor_f7ad4e3d	This strike sends a malware sample known as XZ Backdoor. XZ is a Linux backdoor malware, that is found bundled in the open source compression library XZ Utils. The backdoor leverages a vulnerability, CVE-2024-3094, which utilizes a predefined encrypted private key to run commands on the victim machine as root, if the vulnerable XZ Utils library is installed on the target. The MD5 hash of this XZ Backdoor sample is f7ad4e3d4fd38b84736ac4a365a5db41.
Strike Xamalicious_0ffda3a3	This strike sends a polymorphic malware sample known as Xamalicious. Xamalicious is a sophisticated android backdoor implemented using the Xamarin framework. It employs social engineering to gain accessibility privileges and communicates with a command-and-control server. The second-stage payload, injected dynamically as an assembly DLL, takes full control of the device, potentially engaging in fraudulent activities like ad-clicking and unauthorized financially motivated app installations. 'hello.uwer.hello.hello.google.is.the.best' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 0ffda3a31c5f1ff988a9db7d3195d718.

<b>Name</b>	<b>Description</b>
Strike Xamalicious_41812341	<p>This strike sends a polymorphic malware sample known as Xamalicious. Xamalicious is a sophisticated android backdoor implemented using the Xamarin framework. It employs social engineering to gain accessibility privileges and communicates with a command-and-control server. The second-stage payload, injected dynamically as an assembly DLL, takes full control of the device, potentially engaging in fraudulent activities like ad-clicking and unauthorized financially motivated app installations.</p> <p>'hello.uwer.hello.google.is.the.best' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 418123414126911a089b2f8096265296.</p>
Strike Xamalicious_5e350058	<p>This strike sends a polymorphic malware sample known as Xamalicious. Xamalicious is a sophisticated android backdoor implemented using the Xamarin framework. It employs social engineering to gain accessibility privileges and communicates with a command-and-control server. The second-stage payload, injected dynamically as an assembly DLL, takes full control of the device, potentially engaging in fraudulent activities like ad-clicking and unauthorized financially motivated app installations.</p> <p>'hello.uwer.hello.google.is.the.best' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 5e3500588580f94ce735605c3f03dd34.</p>
Strike Xamalicious_8b4af0f3	<p>This strike sends a polymorphic malware sample known as Xamalicious. Xamalicious is a sophisticated android backdoor implemented using the Xamarin framework. It employs social engineering to gain accessibility privileges and communicates with a command-and-control server. The second-stage payload, injected dynamically as an assembly DLL, takes full control of the device, potentially engaging in fraudulent activities like ad-clicking and unauthorized financially motivated app installations.</p> <p>'hello.uwer.hello.google.is.the.best' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 8b4af0f38cdd44d69fad6f48e168a21c.</p>
Strike Xamalicious_c6e0edb1	<p>This strike sends a malware sample known as Xamalicious. Xamalicious is a sophisticated android backdoor implemented using the Xamarin framework. It employs social engineering to gain accessibility privileges and communicates with a command-and-control server. The second-stage payload, injected dynamically as an assembly DLL, takes full control of the device, potentially engaging in fraudulent activities like ad-clicking and unauthorized financially motivated app installations. 'hello.uwer.hello.google.is.the.best' is the package name of the malware sample. The MD5 hash of this malware sample is c6e0edb1e5b7f163d890f2cc5a3ad273.</p>
Strike Xamalicious_d008d0b2	<p>This strike sends a malware sample known as Xamalicious. Xamalicious is a sophisticated android backdoor implemented using the Xamarin framework. It employs social engineering to gain accessibility privileges and communicates with a command-and-control server. The second-stage payload, injected dynamically as an assembly DLL, takes full control of the device, potentially engaging in fraudulent activities like ad-clicking and unauthorized financially motivated app installations. 'hello.uwer.hello.google.is.the.best' is the package name of the malware sample. The MD5 hash of this malware sample is d008d0b2dbf4c2232903ee28f881be31.</p>

<b>Name</b>	<b>Description</b>
Strike Xamalicious_ef35fa3e	<p>This strike sends a polymorphic malware sample known as Xamalicious. Xamalicious is a sophisticated android backdoor implemented using the Xamarin framework. It employs social engineering to gain accessibility privileges and communicates with a command-and-control server. The second-stage payload, injected dynamically as an assembly DLL, takes full control of the device, potentially engaging in fraudulent activities like ad-clicking and unauthorized financially motivated app installations.</p> <p>'hello.uwer.hello.hello.google.is.the.best' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is ef35fa3e1249c7fb6150cdcb1b8a5c91.</p>
Strike Xamalicious_f72de337	<p>This strike sends a polymorphic malware sample known as Xamalicious. Xamalicious is a sophisticated android backdoor implemented using the Xamarin framework. It employs social engineering to gain accessibility privileges and communicates with a command-and-control server. The second-stage payload, injected dynamically as an assembly DLL, takes full control of the device, potentially engaging in fraudulent activities like ad-clicking and unauthorized financially motivated app installations.</p> <p>'hello.uwer.hello.hello.google.is.the.best' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is f72de33708e41ab8209a362e61437483.</p>
Strike XenomorphV3_8ce057ff	<p>This strike sends an Android malware sample known as Xenomorph V3. The particular sample poses as the Google Play Protect app. It's a sophisticated banking trojan which can extract banking credentials, initiate transactions, obtain 2FA tokens and even transfer funds without any human interaction. 'com.great.calm' is the package name of the malware sample. The MD5 hash of this Xenomorph sample is 8ce057ff57478e98c0e246355ccd27db.</p>
Strike XenomorphV3_a2efff06	<p>This strike sends an Android polymorphic malware sample known as Xenomorph V3. The particular sample poses as the Google Play Protect app. It's a sophisticated banking trojan which can extract banking credentials, initiate transactions, obtain 2FA tokens and even transfer funds without any human interaction. 'com.great.calm' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this Xenomorph sample is a2efff06f0cba69e1363482d189509c3.</p>
Strike XenomorphV3_dd82858b	<p>This strike sends an Android polymorphic malware sample known as Xenomorph V3. The particular sample poses as the Google Play Protect app. It's a sophisticated banking trojan which can extract banking credentials, initiate transactions, obtain 2FA tokens and even transfer funds without any human interaction. 'com.great.calm' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this Xenomorph sample is dd82858bcce2768c354519c831317798.</p>
Strike XtremeRAT_00656070	<p>This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this XtremeRAT sample is 00656070ff12e3f32f13c4d57573ccf8.</p>

<b>Name</b>	<b>Description</b>
Strike XtremeRAT_05d580a8	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this XtremeRAT sample is 05d580a868e5ff141cbf373fbf0bb344.
Strike XtremeRAT_06612bc3	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 06612bc38fd43acf6d3753cada3c3173.
Strike XtremeRAT_08dcdb12	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 08dcdb12e5c8b6a350d7882161704af8.
Strike XtremeRAT_0c36dc4c	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this XtremeRAT sample is 0c36dc4c422bd788d489bb8014cadb6f.
Strike XtremeRAT_0d14a54d	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 0d14a54d8c1a311399fc5ccc4b774b87.
Strike XtremeRAT_0df4f4f5	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 0df4f4f5d006c793efd0cfa500a3e16d.
Strike XtremeRAT_0f8cdbb4	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 0f8cdbb48c4c22ed58b8e64f5c70634b.
Strike XtremeRAT_0f962789	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 0f962789479b1a13385bd6f5b0ef00dc.
Strike XtremeRAT_12699e1c	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 12699e1c7bb1a25472694c32d7f64043.
Strike XtremeRAT_14b71eed	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 14b71eed083794e8794aecdda8a79d26.
Strike XtremeRAT_1589b62e	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has the checksum removed in the PE file format. The MD5 hash of this XtremeRAT sample is 1589b62e89def3d3cc19f8c2b5412e14.

<b>Name</b>	<b>Description</b>
Strike XtremeRAT_193b3d84	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 193b3d8409d629d5562bf50d6880bb27.
Strike XtremeRAT_1a0d960c	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 1a0d960c4a69f9d7d721dada6a12c78c.
Strike XtremeRAT_1a3a8fa2	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 1a3a8fa2a466505c4d4745a2b77091e0.
Strike XtremeRAT_1c84dc95	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 1c84dc95cb7b3b23d2c2fb80b0e1239a.
Strike XtremeRAT_1c8b130f	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 1c8b130f215476a6497cb85e51f92d6b.
Strike XtremeRAT_218be622	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 218be6226719e4ee4e3926b3d9c04442.
Strike XtremeRAT_277609ed	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 277609eeded83e6f042e185c3d5740feb.
Strike XtremeRAT_283b881d	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 283b881d7066550e12fac0a3ff29de5d.
Strike XtremeRAT_2b501d99	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary file has one more imports added in the import table. The MD5 hash of this XtremeRAT sample is 2b501d99f7aa0363c0116b39b34d704d.
Strike XtremeRAT_2b9e53f9	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has random bytes appended at the end of the file. The MD5 hash of this XtremeRAT sample is 2b9e53f9ee6d84137627a127ab07568e.
Strike XtremeRAT_2d2cb797	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this XtremeRAT sample is 2d2cb797b1307d963b45d89d5eb204aa.

<b>Name</b>	<b>Description</b>
Strike XtremeRAT_31c46455	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 31c46455772604a157b0dee4958471ee.
Strike XtremeRAT_31c88bf9	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 31c88bf919e7ef6c1c4cef277d6b5dea.
Strike XtremeRAT_38165906	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 38165906a75593f6a368fa9bb62aed4f.
Strike XtremeRAT_3d08a375	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 3d08a375ab9508a5c5e7da235df6ffad.
Strike XtremeRAT_3e25bcc0	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 3e25bcc06d512252adbcea1b806f2dfc.
Strike XtremeRAT_405d22b5	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 405d22b5eed0d5cf875159b6623ccbaf.
Strike XtremeRAT_44096609	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 44096609059132b91abf2e16adce45c7.
Strike XtremeRAT_440db648	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 440db648da97e821dd5c124708fea7d1.
Strike XtremeRAT_45ac42cd	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 45ac42cd638440f6e2a5df6027615c7e.
Strike XtremeRAT_46f9152b	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 46f9152b680ba99b3ffe3b7235ba6442.
Strike XtremeRAT_521ec057	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 521ec057e179c5f490e5521c0b09bbc9.
Strike XtremeRAT_524e7e63	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 524e7e63d3431e870c08968410412996.

<b>Name</b>	<b>Description</b>
Strike XtremeRAT_5312fb73	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has the timestamp field updated in the PE file header. The MD5 hash of this XtremeRAT sample is 5312fb73c866b581011eb3ab7b89376a.
Strike XtremeRAT_5662944a	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 5662944a31503e9defd62de517dab1d6.
Strike XtremeRAT_58f35ba4	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has the checksum removed in the PE file format. The MD5 hash of this XtremeRAT sample is 58f35ba4608b5371cfeb575026c957af.
Strike XtremeRAT_59777158	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 5977715804652c41a2cb6e606414a0d0.
Strike XtremeRAT_5d057c13	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 5d057c1380096eefa294ffcec51575c1.
Strike XtremeRAT_62f6abc1	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 62f6abc11b6c47327683b8480f9d6f74.
Strike XtremeRAT_6304d5c9	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 6304d5c94ff04ef4de5b6ab20ee482c4.
Strike XtremeRAT_6a1415da	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 6a1415dab169259a084280a25a5b2fdc.
Strike XtremeRAT_7055f299	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has random bytes appended at the end of the file. The MD5 hash of this XtremeRAT sample is 7055f299ca48e6d1a4fa1890d3384b6e.
Strike XtremeRAT_735c5508	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 735c55082d4a6d20db78f44607c35f36.
Strike XtremeRAT_7da04983	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 7da0498327ed786698f533502188c7c4.

<b>Name</b>	<b>Description</b>
Strike XtremeRAT_7e4e41a6	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 7e4e41a6abb7b1ead0dea46ca424b5a7.
Strike XtremeRAT_80908cd8	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 80908cd8528f54634517e0de99af18ce.
Strike XtremeRAT_82384790	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 82384790bea990e94b97cd91ec674b80.
Strike XtremeRAT_893dfc59	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 893dfc59f925b9b05f1a79617e21b124.
Strike XtremeRAT_90a7c094	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 90a7c094e1541e288df6fe17d8af2201.
Strike XtremeRAT_9338a39b	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has random bytes appended at the end of the file. The MD5 hash of this XtremeRAT sample is 9338a39bcc5077aa5b3e42d27624c41e.
Strike XtremeRAT_977f45e5	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 977f45e5cb09032ec6b9cb4a357c40a3.
Strike XtremeRAT_9d72db71	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 9d72db71095177e0bc3e648e53bf5eeb.
Strike XtremeRAT_9e25b902	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 9e25b902a8e0ac18980d5a2cd582ea8d.
Strike XtremeRAT_9eb10374	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has the timestamp field updated in the PE file header. The MD5 hash of this XtremeRAT sample is 9eb103740d2cd929e7fa73be6853be56.
Strike XtremeRAT_9ed68d1b	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is 9ed68d1b2eb4ac8f8e15cf215c6d3253.

<b>Name</b>	<b>Description</b>
Strike XtremeRAT_a0ec57b9	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is a0ec57b95063a067e73958fddd6d834f.
Strike XtremeRAT_a1885beb	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is a1885bebb7c88ac9a4bab04e91c848a5.
Strike XtremeRAT_a1a7174a	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is a1a7174a804d14fc7a8546dae894cd06.
Strike XtremeRAT_a344bf73	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is a344bf734cde979206eeb19372a4acf7.
Strike XtremeRAT_a39ace5e	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is a39ace5e1c16e0ffedbb28e4356606e5.
Strike XtremeRAT_a412baf4	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is a412baf4f612a58b489a66ea9ce819e0.
Strike XtremeRAT_a4ae4668	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is a4ae4668bf4a6b00ce599e24c3d4a9a1.
Strike XtremeRAT_a5b7bad5	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is a5b7bad5f42cf20734060fc7172a68.
Strike XtremeRAT_a67a00f3	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is a67a00f31fa63a762876a35e26548ae0.
Strike XtremeRAT_a6da1059	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is a6da105983786fdcdfbeba004443cb77.
Strike XtremeRAT_a7830f1b	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is a7830f1bfdd4bd60e377f899512117dc.
Strike XtremeRAT_a8502dfa	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is a8502dfaaf19b633bdf35b0058c95ad.

<b>Name</b>	<b>Description</b>
Strike XtremeRAT_a9aae2d6	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is a9aae2d62eb70e5d510072c64eae1d94.
Strike XtremeRAT_a9ec3559	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is a9ec355939ec0234cf7fe1125eae2f7.
Strike XtremeRAT_aa0da4a7	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is aa0da4a762f19d783b2d04392ea23dcf.
Strike XtremeRAT_aa47c1d4	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is aa47c1d468f84c150555a095d08edc88.
Strike XtremeRAT_ab115bd7	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is ab115bd7a7ca4c70c3acbba81ed682e.
Strike XtremeRAT_acf2acc7	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this XtremeRAT sample is acf2acc75f98bd9401c0e31dd438f4f5.
Strike XtremeRAT_ad7baa02	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is ad7baa026ee12f9ca6f0c0f969e9a75c.
Strike XtremeRAT_ae48c84f	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this XtremeRAT sample is ae48c84f07c30348b34aa3c8282589ea.
Strike XtremeRAT_ae5376c6	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is ae5376c64b035c200d4817eb5d01824f.
Strike XtremeRAT_aecd2075	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is aecd2075262f2e69c38eb9c4fc933c80.
Strike XtremeRAT_b5a35b18	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has random bytes appended at the end of the file. The MD5 hash of this XtremeRAT sample is b5a35b1816b34744d602aa0e624a01ac.

<b>Name</b>	<b>Description</b>
Strike XtremeRAT_b6d2a291	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has the timestamp field updated in the PE file header. The MD5 hash of this XtremeRAT sample is b6d2a291d159fc759ffa3631e2f273bf.
Strike XtremeRAT_b7eea26e	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is b7eea26e19f3c867b3e99b1f32be28be.
Strike XtremeRAT_bdbc9286	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is bdbc92863d0b4be83d64cd2003489cc3.
Strike XtremeRAT_bf2b1eb0	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is bf2b1eb048273d25c17913e4990bb4c5.
Strike XtremeRAT_c588e91e	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is c588e91e298577e17cbd22849cb469cf.
Strike XtremeRAT_c7ebcd0d	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has random bytes appended at the end of the file. The MD5 hash of this XtremeRAT sample is c7ebcd0d8c135620ed01f0d5e57deac8.
Strike XtremeRAT_c89afadf	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this XtremeRAT sample is c89afadf76e64097f39455adca932039.
Strike XtremeRAT_cb02045b	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has been packed using upx packer, with the default options. The MD5 hash of this XtremeRAT sample is cb02045b65dd9463c7f06221b77ce1b0.
Strike XtremeRAT_cc0eff29	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is cc0eff29cf999229cb36fb04e9ea5313.
Strike XtremeRAT_cda4d528	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is cda4d52802587e20f29b10ceb14be889.

<b>Name</b>	<b>Description</b>
Strike XtremeRAT_cea8d367	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is cea8d367b150e2afdd38787f15978483.
Strike XtremeRAT_d151b530	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has the checksum removed in the PE file format. The MD5 hash of this XtremeRAT sample is d151b530a789e400bbc89c995cc9103e.
Strike XtremeRAT_d6a934bb	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is d6a934bbc082304cd87bf5091e7829c5.
Strike XtremeRAT_dae76d12	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is dae76d125cf0fbc22ff62143af1c859c.
Strike XtremeRAT_dc6ff189	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this XtremeRAT sample is dc6ff189e58cc7cee002946e3cc635bb.
Strike XtremeRAT_de66d12d	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is de66d12d576a1df764e09f4f51ba1388.
Strike XtremeRAT_e055f8fc	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is e055f8fc8140e42796b541e6e409c71d.
Strike XtremeRAT_e05bc247	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is e05bc247b86c6a2d73bf2519644f41b3.
Strike XtremeRAT_e85a2985	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is e85a2985ba0e39773f1c1a18fe1cab0a.
Strike XtremeRAT_eb27e402	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is eb27e4021af35e509f349581821c0ca4.
Strike XtremeRAT_efc6e7e0	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is efc6e7e02569fc9ac553b6bf19899eeef.

<b>Name</b>	<b>Description</b>
Strike XtremeRAT_ed098eba	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this XtremeRAT sample is ed098eba90e352468dc491acca89ac44.
Strike XtremeRAT_f1cc2d7f	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is f1cc2d7fd58ec1e309bfa09ec55d2fec.
Strike XtremeRAT_f2650149	This strike sends a polymorphic malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this XtremeRAT sample is f2650149885c0116fd8ff232037fdb2f.
Strike XtremeRAT_f2be7da2	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is f2be7da21606a104612fb61f759caa73.
Strike XtremeRAT_f90e0c79	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is f90e0c7971b848a0191aee9f78652f6b.
Strike XtremeRAT_ff40e16f	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is ff40e16f172f69f3ada6b94efd815666.
Strike XtremeRAT_ffa5a03a	This strike sends a malware sample known as XtremeRAT. XtremeRAT is a remote access trojan that allows the attacker to eavesdrop on users and modify the running system. The MD5 hash of this XtremeRAT sample is ffa5a03a9922f642827a9321301848c5.
Strike Zanubis_323d97c8	This strike sends a malware sample known as Zanubis. Zanubis is an Android banking malware that has evolved over the last few years. It employs various obfuscation techniques as well as deceptive tricks to obtain necessary permissions to run. The malware steals data, and sends credentials to a remote C2 server. The MD5 hash of this Zanubis sample is 323d97c876f173628442ff4d1aaa8c98.
Strike Zanubis_45d07497	This strike sends a malware sample known as Zanubis. Zanubis is an Android banking malware that has evolved over the last few years. It employs various obfuscation techniques as well as deceptive tricks to obtain necessary permissions to run. The malware steals data, and sends credentials to a remote C2 server. The MD5 hash of this Zanubis sample is 45d07497ac7fe550b8b394978652caa9.
Strike Zanubis_5c11e88d	This strike sends a malware sample known as Zanubis. Zanubis is an Android banking malware that has evolved over the last few years. It employs various obfuscation techniques as well as deceptive tricks to obtain necessary permissions to run. The malware steals data, and sends credentials to a remote C2 server. The MD5 hash of this Zanubis sample is 5c11e88d1b68a84675af001fd4360068.

<b>Name</b>	<b>Description</b>
Strike Zanubis_660d4eeb	This strike sends a malware sample known as Zanubis. Zanubis is an Android banking malware that has evolved over the last few years. It employs various obfuscation techniques as well as deceptive tricks to obtain necessary permissions to run. The malware steals data, and sends credentials to a remote C2 server. The MD5 hash of this Zanubis sample is 660d4eeb022ee1de93b157e2aa8fe1dc.
Strike Zanubis_6b0d14fb	This strike sends a malware sample known as Zanubis. Zanubis is an Android banking malware that has evolved over the last few years. It employs various obfuscation techniques as well as deceptive tricks to obtain necessary permissions to run. The malware steals data, and sends credentials to a remote C2 server. The MD5 hash of this Zanubis sample is 6b0d14fb1ddd04ac26fb201651eb5070.
Strike Zanubis_7ae448b0	This strike sends a malware sample known as Zanubis. Zanubis is an Android banking malware that has evolved over the last few years. It employs various obfuscation techniques as well as deceptive tricks to obtain necessary permissions to run. The malware steals data, and sends credentials to a remote C2 server. The MD5 hash of this Zanubis sample is 7ae448b067d652f800b0e36b1edea69f.
Strike Zanubis_81f91f20	This strike sends a malware sample known as Zanubis. Zanubis is an Android banking malware that has evolved over the last few years. It employs various obfuscation techniques as well as deceptive tricks to obtain necessary permissions to run. The malware steals data, and sends credentials to a remote C2 server. The MD5 hash of this Zanubis sample is 81f91f201d861e4da765bae8e708c0d0.
Strike Zanubis_8820ab36	This strike sends a malware sample known as Zanubis. Zanubis is an Android banking malware that has evolved over the last few years. It employs various obfuscation techniques as well as deceptive tricks to obtain necessary permissions to run. The malware steals data, and sends credentials to a remote C2 server. The MD5 hash of this Zanubis sample is 8820ab362b7bae6610363d6657c9f788.
Strike Zanubis_8949f492	This strike sends a malware sample known as Zanubis. Zanubis is an Android banking malware that has evolved over the last few years. It employs various obfuscation techniques as well as deceptive tricks to obtain necessary permissions to run. The malware steals data, and sends credentials to a remote C2 server. The MD5 hash of this Zanubis sample is 8949f492001bb0ca9212f85953a6dcda.
Strike Zanubis_90221365	This strike sends a malware sample known as Zanubis. Zanubis is an Android banking malware that has evolved over the last few years. It employs various obfuscation techniques as well as deceptive tricks to obtain necessary permissions to run. The malware steals data, and sends credentials to a remote C2 server. The MD5 hash of this Zanubis sample is 90221365f08640ddcab86a9cd38173ce.
Strike Zanubis_b3f0223e	This strike sends a malware sample known as Zanubis. Zanubis is an Android banking malware that has evolved over the last few years. It employs various obfuscation techniques as well as deceptive tricks to obtain necessary permissions to run. The malware steals data, and sends credentials to a remote C2 server. The MD5 hash of this Zanubis sample is b3f0223e99b7b66a71c2e9b3a0574b12.

<b>Name</b>	<b>Description</b>
Strike Zardoor_07c47f9b	This strike sends a malware sample known as Zardoor. Zardoor is a sophisticated backdoor discovered in a stealthy espionage campaign targeting organizations in the Middle East. This campaign employs custom backdoors and modified reverse proxy tools to establish command and control (C2) and maintain long-term access within victim networks. The threat actor utilizes living-off-the-land binaries (LoLBins) and customized tools to evade detection and execute remote commands. The backdoor transmits encrypted data to attacker's C2, executes fileless PE payloads and updates C2 configuration dynamically. The MD5 hash of this Zardoor sample is 07c47f9b80c3861f219078902b860077.
Strike Zardoor_23f6b621	This strike sends a malware sample known as Zardoor. Zardoor is a sophisticated backdoor discovered in a stealthy espionage campaign targeting organizations in the Middle East. This campaign employs custom backdoors and modified reverse proxy tools to establish command and control (C2) and maintain long-term access within victim networks. The threat actor utilizes living-off-the-land binaries (LoLBins) and customized tools to evade detection and execute remote commands. The backdoor transmits encrypted data to attacker's C2, executes fileless PE payloads and updates C2 configuration dynamically. The MD5 hash of this Zardoor sample is 23f6b621c70024749217614680a2d2b2.
Strike Zardoor_27e96e13	This strike sends a malware sample known as Zardoor. Zardoor is a sophisticated backdoor discovered in a stealthy espionage campaign targeting organizations in the Middle East. This campaign employs custom backdoors and modified reverse proxy tools to establish command and control (C2) and maintain long-term access within victim networks. The threat actor utilizes living-off-the-land binaries (LoLBins) and customized tools to evade detection and execute remote commands. The backdoor transmits encrypted data to attacker's C2, executes fileless PE payloads and updates C2 configuration dynamically. The MD5 hash of this Zardoor sample is 27e96e13a0a538aad23540d52977012f.
Strike Zardoor_3a326ef3	This strike sends a malware sample known as Zardoor. Zardoor is a sophisticated backdoor discovered in a stealthy espionage campaign targeting organizations in the Middle East. This campaign employs custom backdoors and modified reverse proxy tools to establish command and control (C2) and maintain long-term access within victim networks. The threat actor utilizes living-off-the-land binaries (LoLBins) and customized tools to evade detection and execute remote commands. The backdoor transmits encrypted data to attacker's C2, executes fileless PE payloads and updates C2 configuration dynamically. The MD5 hash of this Zardoor sample is 3a326ef320df0d7f111f3a0b27caf238.
Strike Zardoor_72b0ca26	This strike sends a malware sample known as Zardoor. Zardoor is a sophisticated backdoor discovered in a stealthy espionage campaign targeting organizations in the Middle East. This campaign employs custom backdoors and modified reverse proxy tools to establish command and control (C2) and maintain long-term access within victim networks. The threat actor utilizes living-off-the-land binaries (LoLBins) and customized tools to evade detection and execute remote commands. The backdoor transmits encrypted data to attacker's C2, executes fileless PE payloads and updates C2 configuration dynamically. The MD5 hash of this Zardoor sample is 72b0ca267df69ce8c86440a81cd2f321.

<b>Name</b>	<b>Description</b>
Strike Zardoor_82fce2c2	This strike sends a malware sample known as Zardoor. Zardoor is a sophisticated backdoor discovered in a stealthy espionage campaign targeting organizations in the Middle East. This campaign employs custom backdoors and modified reverse proxy tools to establish command and control (C2) and maintain long-term access within victim networks. The threat actor utilizes living-off-the-land binaries (LoLBins) and customized tools to evade detection and execute remote commands. The backdoor transmits encrypted data to attacker's C2, executes fileless PE payloads and updates C2 configuration dynamically. The MD5 hash of this Zardoor sample is 82fce2c2a557e1580c82c9c7e15a8c79.
Strike Zardoor_91a53364	This strike sends a malware sample known as Zardoor. Zardoor is a sophisticated backdoor discovered in a stealthy espionage campaign targeting organizations in the Middle East. This campaign employs custom backdoors and modified reverse proxy tools to establish command and control (C2) and maintain long-term access within victim networks. The threat actor utilizes living-off-the-land binaries (LoLBins) and customized tools to evade detection and execute remote commands. The backdoor transmits encrypted data to attacker's C2, executes fileless PE payloads and updates C2 configuration dynamically. The MD5 hash of this Zardoor sample is 91a533644f0a1440c82572b563d9eed9.
Strike Zardoor_dd5694d0	This strike sends a malware sample known as Zardoor. Zardoor is a sophisticated backdoor discovered in a stealthy espionage campaign targeting organizations in the Middle East. This campaign employs custom backdoors and modified reverse proxy tools to establish command and control (C2) and maintain long-term access within victim networks. The threat actor utilizes living-off-the-land binaries (LoLBins) and customized tools to evade detection and execute remote commands. The backdoor transmits encrypted data to attacker's C2, executes fileless PE payloads and updates C2 configuration dynamically. The MD5 hash of this Zardoor sample is dd5694d0797e22f521faeb6026eddaa8.
Strike Zardoor_dffa48f2	This strike sends a malware sample known as Zardoor. Zardoor is a sophisticated backdoor discovered in a stealthy espionage campaign targeting organizations in the Middle East. This campaign employs custom backdoors and modified reverse proxy tools to establish command and control (C2) and maintain long-term access within victim networks. The threat actor utilizes living-off-the-land binaries (LoLBins) and customized tools to evade detection and execute remote commands. The backdoor transmits encrypted data to attacker's C2, executes fileless PE payloads and updates C2 configuration dynamically. The MD5 hash of this Zardoor sample is dffa48f29a363071d47ffd114545009.
Strike Zardoor_e0f4afe3	This strike sends a malware sample known as Zardoor. Zardoor is a sophisticated backdoor discovered in a stealthy espionage campaign targeting organizations in the Middle East. This campaign employs custom backdoors and modified reverse proxy tools to establish command and control (C2) and maintain long-term access within victim networks. The threat actor utilizes living-off-the-land binaries (LoLBins) and customized tools to evade detection and execute remote commands. The backdoor transmits encrypted data to attacker's C2, executes fileless PE payloads and updates C2 configuration dynamically. The MD5 hash of this Zardoor sample is e0f4afe374d75608d604fbf108eac64f.

<b>Name</b>	<b>Description</b>
Strike Zardoor_eb8d418c	This strike sends a malware sample known as Zardoor. Zardoor is a sophisticated backdoor discovered in a stealthy espionage campaign targeting organizations in the Middle East. This campaign employs custom backdoors and modified reverse proxy tools to establish command and control (C2) and maintain long-term access within victim networks. The threat actor utilizes living-off-the-land binaries (LoLBins) and customized tools to evade detection and execute remote commands. The backdoor transmits encrypted data to attacker's C2, executes fileless PE payloads and updates C2 configuration dynamically. The MD5 hash of this Zardoor sample is eb8d418c036b00e4381671bf67c2e1b0.
Strike Zbot_0262db6c	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is 0262db6c1bd924b0718f7957c7e18a0c.
Strike Zbot_13899a88	This strike sends a polymorphic malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Zbot sample is 13899a886a4d9dec340f4c976203ce2a.
Strike Zbot_26f59367	This strike sends a polymorphic malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has been packed using upx packer, with the default options. The MD5 hash of this Zbot sample is 26f593677b2cca80b74d2195ca3255e6.
Strike Zbot_376b9a6c	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is 376b9a6c75d6c7da8dc7c0e21338f7f4.
Strike Zbot_45fca4d6	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is 45fca4d6d8f0649b29b475a6ca4eb6cb.
Strike Zbot_46800190	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is 46800190931451e5cae956f112696a64.
Strike Zbot_4a245548	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is 4a24554855308b574ae2327d733fc1f6.
Strike Zbot_53398513	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is 53398513c9b00ac5c9e11bc0ac41d1b6.
Strike Zbot_68a18f08	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is 68a18f089ca381727f149f727d03193e.

<b>Name</b>	<b>Description</b>
Strike Zbot_7fffd12	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is 7fffd12a34a3016695ee2de18e9d387.
Strike Zbot_80a79ad8	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is 80a79ad839870daeb6b3bce92d25b9cd.
Strike Zbot_8ebb01a1	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is 8ebb01a18e6a4766213809c2de63a5b1.
Strike Zbot_8fd8d53c	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is 8fd8d53c05e3b556917a507ed6ec6b48.
Strike Zbot_a26f582f	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is a26f582f48d3b9f65e57254df0e6a3c1.
Strike Zbot_ae999d4e	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is ae999d4ee4684b297f66ffea7c38f611.
Strike Zbot_b67643a6	This strike sends a polymorphic malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Zbot sample is b67643a6adadf9d104309476df6e7234.
Strike Zbot_c76096dd	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is c76096ddd9e001457bd5f9a688e577f1.
Strike Zbot_d87c8524	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is d87c85244e51ed71b942fff9a15158a4.
Strike Zbot_e14e0d98	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is e14e0d98cfbdca65f37e7d1fa1448d33.
Strike Zbot_e285f10c	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is e285f10c95c30b4807282c16269dbb33.
Strike Zbot_e51be375	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is e51be375b6b37bc31fb815e35e8fa238.

<b>Name</b>	<b>Description</b>
Strike Zbot_fe2e0db4	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is fe2e0db42c21c90dcdbbe0983ab89276.
Strike Zbot_fe56fc37	This strike sends a malware sample known as Zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this Zbot sample is fe56fc379bd393a225923b588e3ce27b.
Strike Zegost_02293aea	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 02293aead10c7195514fbbaa749ee2dd.
Strike Zegost_0408ff2a	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 0408ff2a2f67c7492a269a9a7d71b980.
Strike Zegost_06e1716a	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 06e1716af034046c88874d7d338afbe9.
Strike Zegost_09e295bd	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 09e295bd6b7c1d6714e107f28e5414f5.
Strike Zegost_0a9281d4	This strike sends a polymorphic malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Zegost sample is 0a9281d4c468831b6b946d43d2ebf16f.
Strike Zegost_10d7b4f7	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 10d7b4f78c61a60f124b65233b2dd6c2.
Strike Zegost_114a0086	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zegost sample is 114a00861438a53af3626629f072c496.

<b>Name</b>	<b>Description</b>
Strike Zegost_1c449492	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zegost sample is 1c4494926a2b2555a13753a528bca733.
Strike Zegost_1cf31a4e	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 1cf31a4eed8b843df39342fb99984f24.
Strike Zegost_1d15f5f9	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 1d15f5f9360c8f1e3f1f871401f6599f.
Strike Zegost_1e5b1708	This strike sends a polymorphic malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Zegost sample is 1e5b1708147129aba1f46ffeae389376.
Strike Zegost_21be8e77	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 21be8e778089b7bcd8b9ab9b26197a6.
Strike Zegost_2609f845	This strike sends a polymorphic malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Zegost sample is 2609f845507a4ae9a9d2a32016498630.
Strike Zegost_28ae85d8	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 28ae85d88fed2184bba78d1af16827da.
Strike Zegost_2a361689	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 2a361689bd76bb804dc4f9b2088c152f.
Strike Zegost_2e7bc9b2	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 2e7bc9b2ca377b14f5cb26fc719792db.

<b>Name</b>	<b>Description</b>
Strike Zegost_3ec0f08b	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 3ec0f08b9a5e8cd350d60ea98b66bc6b.
Strike Zegost_41c3eb41	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 41c3eb4117d78836fa43acbb3fd1a362.
Strike Zegost_461c6d64	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 461c6d648ad38eaf49feb08a5f7a34d8.
Strike Zegost_46762216	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zegost sample is 4676221611d727a8b2c54f6e78da92ee.
Strike Zegost_4b186588	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zegost sample is 4b186588668a181de87fd5520bf57219.
Strike Zegost_582433da	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zegost sample is 582433da271d3f4c78027bbebba4e4c.
Strike Zegost_5bbc6e17	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 5bbc6e178e98a48301ba1c78671c89e5.
Strike Zegost_5bde8a69	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zegost sample is 5bde8a697c4ed4b020035278f48ebbca.
Strike Zegost_5c6ef7c4	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 5c6ef7c40c341feec5ef105b2bea417c.

<b>Name</b>	<b>Description</b>
Strike Zegost_5d8c75df	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 5d8c75dfa07e5982d2d90a282378e4cb.
Strike Zegost_5f51017f	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zegost sample is 5f51017f19491c2ac494eff70ea30279.
Strike Zegost_6538e4c9	This strike sends a polymorphic malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this Zegost sample is 6538e4c9b1665b2aa256b625e2fb9fa2.
Strike Zegost_67539483	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 6753948390a4c7be1624520222b28b58.
Strike Zegost_6c6181b4	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 6c6181b4a564254c0d5f16512632660c.
Strike Zegost_6da73d62	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 6da73d62e3ad95ae34801c12a79e113f.
Strike Zegost_72ab4d3f	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 72ab4d3f08f9136464836d4b0d633ba3.
Strike Zegost_88ae879a	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zegost sample is 88ae879afdc027bcb823d51dbb777d15.
Strike Zegost_9d4c308c	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is 9d4c308c78451e878ba18901b4a0df90.

<b>Name</b>	<b>Description</b>
Strike Zegost_9f52a0f4	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zegost sample is 9f52a0f4981acda5629b4281651eba9f.
Strike Zegost_a69a7a2e	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is a69a7a2eea907b80dd34b110efe6f09a.
Strike Zegost_ac8f541f	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is ac8f541ff183fc73e5a64b212ef95fff.
Strike Zegost_b4d81bd7	This strike sends a polymorphic malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The binary has been packed using upx packer, with the default options. The MD5 hash of this Zegost sample is b4d81bd727d1b0f197e83dfe045147f0.
Strike Zegost_c705646b	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is c705646bd19311dd646cc5c71a403e71.
Strike Zegost_c9c948c0	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is c9c948c02a6cb14c046f9497e66196fb.
Strike Zegost_d095518b	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is d095518bd11c6a6bb8737ae42a26fe4b.
Strike Zegost_d115a6dc	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is d115a6dc468be0e6dcba2421c88c2231e.
Strike Zegost_d9d34b56	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zegost sample is d9d34b56a18544feb9acbca806cfad7.

<b>Name</b>	<b>Description</b>
Strike Zegost_e12b647e	This strike sends a polymorphic malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The binary has the checksum removed in the PE file format. The MD5 hash of this Zegost sample is e12b647e05df25b0a8d0ec89c409969e.
Strike Zegost_e4fb9690	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zegost sample is e4fb9690e4d9fdf344b73d4196c18ef3.
Strike Zegost_e8bea4b9	This strike sends a polymorphic malware sample known as Zegost. Zegost, also known as Zusy, uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe". When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The binary has random bytes appended at the end of the file. The MD5 hash of this Zegost sample is e8bea4b97c08b5123088e99497c4cdc7.
Strike Zegost_eac003a4	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is eac003a405c720f1070d3fd2eaeed11d.
Strike Zegost_eaddbf2d	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is eaddbf2d17a8e690a58e195e35451222.
Strike Zegost_f9e8a2f9	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is f9e8a2f913ea31aba2f95c04f997e12d.
Strike Zegost_fb967cd2	This strike sends a malware sample known as Zegost. Zegost, also known as Zusy, steals banking information. It displays a form to trick the user into submitting personal information when visiting a banking website. The MD5 hash of this Zegost sample is fb967cd2599061cb0a3dab0cade0fc3c.
Strike ZeroAccess_079c063f	This strike sends a polymorphic malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The binary has random bytes appended at the end of the file. The MD5 hash of this ZeroAccess sample is 079c063f97182ef3c31dfa5707c9909f.

<b>Name</b>	<b>Description</b>
Strike ZeroAccess_0d6be0ae	This strike sends a polymorphic malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The binary has random bytes appended at the end of the file. The MD5 hash of this ZeroAccess sample is 0d6be0aedd9217ecd67e329f37479768.
Strike ZeroAccess_11451aa1	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 11451aa12c105af614f8271381983400.
Strike ZeroAccess_194fc911	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 194fc911595fb4024d0e008946ec6b18.
Strike ZeroAccess_1b80880f	This strike sends a polymorphic malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this ZeroAccess sample is 1b80880fd0c401f7a25e47e56105cf7b.
Strike ZeroAccess_218c68ce	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 218c68ce147d4b49365e643806d0b1cb.
Strike ZeroAccess_2d3ecd00	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 2d3ecd0011581f113735ffd46ef8fc22.
Strike ZeroAccess_353353e7	This strike sends a polymorphic malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this ZeroAccess sample is 353353e771ca42fea2cb01005485fd8f.
Strike ZeroAccess_3a328207	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 3a3282073f5d36d0e2edd18fa20bcb5d.
Strike ZeroAccess_49158788	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 49158788220d59f7692de831f7e64175.

<b>Name</b>	<b>Description</b>
Strike ZeroAccess_49570ea4	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 49570ea4a11bb82d2ae773164f58c04.
Strike ZeroAccess_4c6089f9	This strike sends a polymorphic malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this ZeroAccess sample is 4c6089f91462f9f07d0de266688420e1.
Strike ZeroAccess_51d0091f	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 51d0091fd150543df73799749056996f.
Strike ZeroAccess_539f9f37	This strike sends a polymorphic malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this ZeroAccess sample is 539f9f377347a58ffde24c5bf659697b.
Strike ZeroAccess_55d36baa	This strike sends a polymorphic malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The binary has the checksum removed in the PE file format. The MD5 hash of this ZeroAccess sample is 55d36baac8bea015ef59279f331b6c88.
Strike ZeroAccess_569b2af9	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 569b2af985cb1f4b9b368444889d13c4.
Strike ZeroAccess_5752712f	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 5752712ff20c633b34db7207cee893d2.
Strike ZeroAccess_7dbfa1f4	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 7dbfa1f42d8fb465ebdf98f564196984.
Strike ZeroAccess_8426c0cf	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 8426c0cfafec261c69b5c08d63724c70.

<b>Name</b>	<b>Description</b>
Strike ZeroAccess_8f15b013	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 8f15b0136b3fbc214755ac1fa2f3347e.
Strike ZeroAccess_95ddece9	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 95ddece98d72b8ef206cbcdeb9436653.
Strike ZeroAccess_98f3a2ab	This strike sends a polymorphic malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The binary has the timestamp field updated in the PE file header. The MD5 hash of this ZeroAccess sample is 98f3a2ab6191279de94de7a956c53dc5.
Strike ZeroAccess_9aa64232	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 9aa64232ca7425b4831bb10687293399.
Strike ZeroAccess_9be94e1a	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 9be94e1ac5349f1265c0627b48fd0fa6.
Strike ZeroAccess_9ea002e2	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is 9ea002e2ac906ab1aeaa2c85486955bd.
Strike ZeroAccess_b2401b9b	This strike sends a polymorphic malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The binary has the checksum removed in the PE file format. The MD5 hash of this ZeroAccess sample is b2401b9b875c7259ca8ed1b833c63dea.
Strike ZeroAccess_b5b0b385	This strike sends a polymorphic malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this ZeroAccess sample is b5b0b385842df2d28e13532b05996e7b.
Strike ZeroAccess_ba15b25f	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is ba15b25f7eac496cc69525ac079338ff.

<b>Name</b>	<b>Description</b>
Strike ZeroAccess_c352fae2	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is c352fae2894124a4c4e7e9c5ff99f8e5.
Strike ZeroAccess_c4c69c5a	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is c4c69c5acd63a6d9be8c893b56b43434.
Strike ZeroAccess_c4e7f9c9	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is c4e7f9c9224801d1811880efb64d1398.
Strike ZeroAccess_cba44d1a	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is cba44d1ad8632bbc2beccf7ff27b743e.
Strike ZeroAccess_e30a52b5	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is e30a52b5e3ba0ead21a352895e02f83a.
Strike ZeroAccess_e8a0eeaf	This strike sends a polymorphic malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The binary has the timestamp field updated in the PE file header. The MD5 hash of this ZeroAccess sample is e8a0eeaf2c2ef871660694530020cec6.
Strike ZeroAccess_ff795bd8	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is ff795bd814b0102b9d01ebd74b1f2b9b.
Strike ZeroAccess_ffd533f2	This strike sends a malware sample known as ZeroAccess. ZeroAccess is a trojan that infects Windows systems, installing a rootkit to hide its presence on the affected machine and serves as a platform for conducting click-fraud campaigns. The MD5 hash of this ZeroAccess sample is ffd533f2f95fa70144abf171e18665de.
Strike Zeus_03a4b7f3	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 03a4b7f3f55b57f772d2ff874447ffbf.
Strike Zeus_04ee0e76	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 04ee0e7627ef287ef9da9c24d070dc6e.

<b>Name</b>	<b>Description</b>
Strike Zeus_07c496de	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 07c496defd5a1aae99144c230162f4df.
Strike Zeus_0da65917	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 0da65917d86216639bb6c3a43b18ae26.
Strike Zeus_0e9c672e	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 0e9c672e99ee2776c07c114bbeaf83c.
Strike Zeus_14a50168	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 14a50168b16aee6a819b135c941524d6.
Strike Zeus_14fbc383	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 14fbc38315011e6444caf46d257450df.
Strike Zeus_18055f9d	This strike sends a polymorphic malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The binary has the timestamp field updated in the PE file header. The MD5 hash of this Zeus sample is 18055f9dea82d5a3680d6c3740abffa1.
Strike Zeus_1c34aea8	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 1c34aea84be6566df0e0e19b4b089d48.
Strike Zeus_1d7353bf	This strike sends a polymorphic malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The binary has been packed using upx packer, with the default options. The MD5 hash of this Zeus sample is 1d7353bf37c850c5a72c8705aa1a5a7c.
Strike Zeus_20191b6f	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 20191b6f64ae1103944aa2e149ddda1b.
Strike Zeus_2301cfe5	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 2301cfe5e49029d6c880aea8fe980ef0.
Strike Zeus_2455d1e7	This strike sends a polymorphic malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The binary has random bytes appended at the end of the file. The MD5 hash of this Zeus sample is 2455d1e77f1c4d608580fab08cb1b23a.

<b>Name</b>	<b>Description</b>
Strike Zeus_2da29c85	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 2da29c85052f458428e01873526fd980.
Strike Zeus_3166efa8	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 3166efa8e6a246c300786b4d38534337.
Strike Zeus_321c05db	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 321c05db1742f2ff52e9ef49863cbe0b.
Strike Zeus_3a86f38c	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 3a86f38c6f43ab954120c16432b4add7.
Strike Zeus_3e3725ab	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 3e3725aba8ea8e5aaeaceccb455284ba.
Strike Zeus_42cb8302	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 42cb830206b6d47bec1f1d2569ee5412.
Strike Zeus_481cf179	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 481cf1793f80b3a9feb66d74d22ef16a.
Strike Zeus_48cda006	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 48cda006baf5e9d224fe0a8ed0e84462.
Strike Zeus_48ed6900	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 48ed690087909f90004d251a36868f5c.
Strike Zeus_4c7160a8	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 4c7160a88e93b63f9d9e178e9d91d028.
Strike Zeus_61762e53	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 61762e53a4565d35bcadf0feb5ebb161.
Strike Zeus_62075219	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 6207521970ad9c1f9edca5f37ae9955c.

<b>Name</b>	<b>Description</b>
Strike Zeus_64fd15df	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 64fd15df41586ee7d8e036d4cc9da625.
Strike Zeus_690584c6	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 690584c6705200db811833404401d530.
Strike Zeus_6a6e60c6	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 6a6e60c6e1562053632860bcef8e3b4a.
Strike Zeus_719738a1	This strike sends a polymorphic malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The binary has been packed using upx packer, with the default options. The MD5 hash of this Zeus sample is 719738a162dcfd5189e22543125cdd0a.
Strike Zeus_77cd76d7	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 77cd76d73312c2d123d03d37150eb52d.
Strike Zeus_78e8ac87	This strike sends a polymorphic malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this Zeus sample is 78e8ac87e15e2e6dbf1d42a2e5a7e547.
Strike Zeus_84712478	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 847124780a7d2ac548d331d061a1eaaa.
Strike Zeus_86bf4400	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 86bf4400ae301e2d2b734441e91fb61.
Strike Zeus_902e65b4	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 902e65b42621a37991cf902404940aa7.
Strike Zeus_9cae42d1	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 9cae42d10b031fb94a730935859b8123.
Strike Zeus_9d5a2929	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is 9d5a2929fd17bb8f5a0233592834762c.

<b>Name</b>	<b>Description</b>
Strike Zeus_a3e87757	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is a3e877574325cec92a586354a024f568.
Strike Zeus_a5d0e7b6	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is a5d0e7b631a433cc6ab9648e7887682d.
Strike Zeus_a74f8bab	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is a74f8bab71709858b2d97f91777d23f8.
Strike Zeus_a7b44399	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is a7b44399bc29f4df8de7aab5e6d8b6db.
Strike Zeus_ade5bccc	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is ade5bccc77af766b64964bd007b8e353.
Strike Zeus_b0bfdd56	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is b0bfdd56f77021b5d31a4c9f0c778e8c.
Strike Zeus_b2f96198	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is b2f9619812c7c91431546b7ee6f13139.
Strike Zeus_b7f9e5b5	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is b7f9e5b596ca5e2262e14e39559f418f.
Strike Zeus_b9a978e2	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is b9a978e2c2d020973e9fb45464861736.
Strike Zeus_b9aa1d42	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is b9aa1d424a4625782147f2bacea153f0.
Strike Zeus_beb707ac	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is beb707aca799fd96795ac701ac2dcd60.
Strike Zeus_c0eeab2a	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is c0eeab2a49bd4f96ef8b52a122879370.

<b>Name</b>	<b>Description</b>
Strike Zeus_c79ba332	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is c79ba3328e3754cae49e425b95ad05804.
Strike Zeus_d345dcea	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is d345dcea72356a1e8335c227d6a0a791.
Strike Zeus_d64f8682	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is d64f868269ec5a07a22779bc970f0588.
Strike Zeus_d7e76f37	This strike sends a polymorphic malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this Zeus sample is d7e76f3798e003fa9dbe5474ac1f18ea.
Strike Zeus_d94a1caf	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is d94a1caf3030acd2c4afa905cb973361.
Strike Zeus_ea340932	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is ea340932ae2e3fb0b249a1c54378227.
Strike Zeus_ec2c4be6	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is ec2c4be68d2eb0048cfda4d85c287e90.
Strike Zeus_ec9230ca	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is ec9230ca382c5c5ce887b292d010e92e.
Strike Zeus_f7504799	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is f7504799f08db3c40c08b80d5c2f1c9f.
Strike Zeus_f97fc586	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is f97fc586a65bcfa4948fbaef03e933a5.
Strike Zeus_faaaade2	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is faaaade25f3ce28be571087adbce55d5.
Strike Zeus_ffb5d7b3	This strike sends a malware sample known as Zeus. Zeus is a trojan that steals information such as banking credentials using methods such as key-logging and form-grabbing. The MD5 hash of this Zeus sample is ffb5d7b3e1829fc08e5cb9e68e3fe3af.

<b>Name</b>	<b>Description</b>
Strike ZuoRAT Router Sample_1a9d8467	This strike sends a malware sample known as ZuoRAT Router Sample. ZuoRAT is malware that targets SOHO routers that enumerates the host and LAN, and can capture network packets being transmitted over the infected device. The MD5 hash of this ZuoRAT Router Sample sample is 1a9d8467424e30741a661d134828299c.
Strike ZuoRAT Router Sample_bbc2c916	This strike sends a malware sample known as ZuoRAT Router Sample. ZuoRAT is malware that targets SOHO routers that enumerates the host and LAN, and can capture network packets being transmitted over the infected device. The MD5 hash of this ZuoRAT Router Sample sample is bbc2c916dc7cd30b389ff423a325fd74.
Strike ZuoRAT Windows Loader_127ccc1b	This strike sends a malware sample known as ZuoRAT Windows Loader. The ZuoRAT Windows loader is used to retrieve a remote 2nd stage payload and load it on the Windows machine. It deploys either the CBeacon, GoBeacon, or Cobalt Strike trojans. The MD5 hash of this ZuoRAT Windows Loader sample is 127ccc1b4363eb1639af1baf372984e3.
Strike ZuoRAT Windows Loader_1fdb045e	This strike sends a malware sample known as ZuoRAT Windows Loader. The ZuoRAT Windows loader is used to retrieve a remote 2nd stage payload and load it on the Windows machine. It deploys either the CBeacon, GoBeacon, or Cobalt Strike trojans. The MD5 hash of this ZuoRAT Windows Loader sample is 1fdb045ed27c7f24109a9783fe570db4.
Strike ZuoRAT Windows Loader_20e463d3	This strike sends a malware sample known as ZuoRAT Windows Loader. The ZuoRAT Windows loader is used to retrieve a remote 2nd stage payload and load it on the Windows machine. It deploys either the CBeacon, GoBeacon, or Cobalt Strike trojans. The MD5 hash of this ZuoRAT Windows Loader sample is 20e463d3b1d53bc4d64ae7e679559f7c.
Strike ZuoRAT Windows Loader_29cdc592	This strike sends a malware sample known as ZuoRAT Windows Loader. The ZuoRAT Windows loader is used to retrieve a remote 2nd stage payload and load it on the Windows machine. It deploys either the CBeacon, GoBeacon, or Cobalt Strike trojans. The MD5 hash of this ZuoRAT Windows Loader sample is 29cdc592f4f8bab3fbc04b04b12c91ab.
Strike ZuoRAT Windows Loader_385cd8dc	This strike sends a malware sample known as ZuoRAT Windows Loader. The ZuoRAT Windows loader is used to retrieve a remote 2nd stage payload and load it on the Windows machine. It deploys either the CBeacon, GoBeacon, or Cobalt Strike trojans. The MD5 hash of this ZuoRAT Windows Loader sample is 385cd8dcec1907d12f42798fc93158da.
Strike ZuoRAT Windows Loader_3ea67bfd	This strike sends a malware sample known as ZuoRAT Windows Loader. The ZuoRAT Windows loader is used to retrieve a remote 2nd stage payload and load it on the Windows machine. It deploys either the CBeacon, GoBeacon, or Cobalt Strike trojans. The MD5 hash of this ZuoRAT Windows Loader sample is 3ea67bfd0c11ee51d036635ab1aee93a.
Strike ZuoRAT Windows Loader_800c2828	This strike sends a malware sample known as ZuoRAT Windows Loader. The ZuoRAT Windows loader is used to retrieve a remote 2nd stage payload and load it on the Windows machine. It deploys either the CBeacon, GoBeacon, or Cobalt Strike trojans. The MD5 hash of this ZuoRAT Windows Loader sample is 800c2828450a33c3b879f9f51dbdd98a.

<b>Name</b>	<b>Description</b>
Strike ZuoRAT Windows Loader_8325322a	This strike sends a malware sample known as ZuoRAT Windows Loader. The ZuoRAT Windows loader is used to retrieve a remote 2nd stage payload and load it on the Windows machine. It deploys either the CBeacon, GoBeacon, or Cobalt Strike trojans. The MD5 hash of this ZuoRAT Windows Loader sample is 8325322a8db4c6cdb2544792253b2bf1.
Strike ZuoRAT Windows Loader_9b07d1b4	This strike sends a malware sample known as ZuoRAT Windows Loader. The ZuoRAT Windows loader is used to retrieve a remote 2nd stage payload and load it on the Windows machine. It deploys either the CBeacon, GoBeacon, or Cobalt Strike trojans. The MD5 hash of this ZuoRAT Windows Loader sample is 9b07d1b4acaad080c5e68411b9072e9.
Strike ZuoRAT Windows Loader_c32ccfa7	This strike sends a malware sample known as ZuoRAT Windows Loader. The ZuoRAT Windows loader is used to retrieve a remote 2nd stage payload and load it on the Windows machine. It deploys either the CBeacon, GoBeacon, or Cobalt Strike trojans. The MD5 hash of this ZuoRAT Windows Loader sample is c32ccfa73f4a13972a447ccde1041950.
Strike Zusy_041d343d	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 041d343d2c16b009b6b5cd1612feae3c.
Strike Zusy_07b49a96	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 07b49a968feacfa06f404be79213efce.
Strike Zusy_0c2339be	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 0c2339bed4022b2a2d241f14852eb426.
Strike Zusy_0ddad360	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 0ddad3606a7b0a0edf9220d1fe6a340b.

<b>Name</b>	<b>Description</b>
Strike Zusy_32c78bb6	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 32c78bb6fafc6c41a529ba89f169d84f.
Strike Zusy_355c4601	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 355c4601a27a7a4b62b75b9ca171e6bf.
Strike Zusy_3c720563	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 3c720563ec1c728ad4f8646c2b991d17.
Strike Zusy_3d1be4d0	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 3d1be4d0b627ed1a301848bddfdbcc98.
Strike Zusy_47b78fd0	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 47b78fd02008e19783fd85846662b278.
Strike Zusy_4b742a09	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 4b742a093c100801a449d3fb2b040b85.
Strike Zusy_747cc78c	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 747cc78c975baa2992b25d27838f2d46.

<b>Name</b>	<b>Description</b>
Strike Zusy_75cad729	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 75cad729ca6a900e3b169f3b8376fb23.
Strike Zusy_8e730c2e	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 8e730c2ea7244f28a948842fbe6f094a.
Strike Zusy_90afa5f3	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 90afa5f30c43d1968de6d9e3202ae7d2.
Strike Zusy_9a973d35	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is 9a973d3584fcc63bb12b28f2048da7af.
Strike Zusy_be37ac96	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is be37ac96a8cb08a2184662e533b5f5e4.
Strike Zusy_cba5b2bb	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is cba5b2bb7a701a6900a05c75ff171e9e.
Strike Zusy_d586ef3d	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is d586ef3d3ce938f2b02e8e6ee0d2c1a0.

<b>Name</b>	<b>Description</b>
Strike Zusy_f94938b4	This strike sends a malware sample known as Zusy. Zusy, also known as TinyBanker or Tinba, is a trojan that uses man-in-the-middle attacks to steal banking information. When executed, it injects itself into legitimate Windows processes such as "explorer.exe" and "winver.exe." When the user accesses a banking website, it displays a form to trick the user into submitting personal information. The MD5 hash of this Zusy sample is f94938b4aae9ff3f4dc976d3f8dd50fc.
Strike androidrat_5a2cf637	This strike sends a polymorphic malware sample known as Android RAT. This malware is an Android Remote Access Trojan (RAT) designed to steal credentials. The malware masquerades as popular Android apps and, once installed, requests accessibility and device admin permissions to control the device. It communicates with a command-and-control server to receive instructions for various malicious activities, including reading messages and call logs, sending SMS, toggling the camera flashlight, and opening phishing URLs in a browser. 'sigma.male' is the package name of the malware sample. Constant strings in the code has been encrypted. The MD5 hash of this malware sample is 5a2cf63779dca296193fc3e701971788.
Strike androidrat_675f8d75	This strike sends a polymorphic malware sample known as Android RAT. This malware is an Android Remote Access Trojan (RAT) designed to steal credentials. The malware masquerades as popular Android apps and, once installed, requests accessibility and device admin permissions to control the device. It communicates with a command-and-control server to receive instructions for various malicious activities, including reading messages and call logs, sending SMS, toggling the camera flashlight, and opening phishing URLs in a browser. 'sigma.male' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 675f8d7524200292d6eadf8b7a1e65bf.
Strike androidrat_a2e31db4	This strike sends a polymorphic malware sample known as Android RAT. This malware is an Android Remote Access Trojan (RAT) designed to steal credentials. The malware masquerades as popular Android apps and, once installed, requests accessibility and device admin permissions to control the device. It communicates with a command-and-control server to receive instructions for various malicious activities, including reading messages and call logs, sending SMS, toggling the camera flashlight, and opening phishing URLs in a browser. 'sigma.male' is the package name of the malware sample. Constant strings in the code has been encrypted. The MD5 hash of this malware sample is a2e31db4970e4261dccd5ef0501eed90.
Strike androidrat_cb44ee4c	This strike sends a malware sample known as Android RAT. This malware is an Android Remote Access Trojan (RAT) designed to steal credentials. The malware masquerades as popular Android apps and, once installed, requests accessibility and device admin permissions to control the device. It communicates with a command-and-control server to receive instructions for various malicious activities, including reading messages and call logs, sending SMS, toggling the camera flashlight, and opening phishing URLs in a browser. 'sigma.male' is the package name of the malware sample. The MD5 hash of this malware sample is cb44ee4cbdbbefcad5c20324af7dfd72.

Name	Description
Strike androidrat_d9939468	This strike sends a polymorphic malware sample known as Android RAT. This malware is an Android Remote Access Trojan (RAT) designed to steal credentials. The malware masquerades as popular Android apps and, once installed, requests accessibility and device admin permissions to control the device. It communicates with a command-and-control server to receive instructions for various malicious activities, including reading messages and call logs, sending SMS, toggling the camera flashlight, and opening phishing URLs in a browser. 'sigma.male' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is d9939468237afc8f8bc4ecaee13ae740.
Strike androidrat_db9efbae	This strike sends a malware sample known as Android RAT. This malware is an Android Remote Access Trojan (RAT) designed to steal credentials. The malware masquerades as popular Android apps and, once installed, requests accessibility and device admin permissions to control the device. It communicates with a command-and-control server to receive instructions for various malicious activities, including reading messages and call logs, sending SMS, toggling the camera flashlight, and opening phishing URLs in a browser. 'sigma.male' is the package name of the malware sample. The MD5 hash of this malware sample is db9efbaeed892b82f46666b669f27c90.
Strike androidrat_f115c6b5	This strike sends a polymorphic malware sample known as Android RAT. This malware is an Android Remote Access Trojan (RAT) designed to steal credentials. The malware masquerades as popular Android apps and, once installed, requests accessibility and device admin permissions to control the device. It communicates with a command-and-control server to receive instructions for various malicious activities, including reading messages and call logs, sending SMS, toggling the camera flashlight, and opening phishing URLs in a browser. 'sigma.male' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is f115c6b5d47ce8bc3b978f68a995a572.
Strike androidrat_f881565d	This strike sends a polymorphic malware sample known as Android RAT. This malware is an Android Remote Access Trojan (RAT) designed to steal credentials. The malware masquerades as popular Android apps and, once installed, requests accessibility and device admin permissions to control the device. It communicates with a command-and-control server to receive instructions for various malicious activities, including reading messages and call logs, sending SMS, toggling the camera flashlight, and opening phishing URLs in a browser. 'sigma.male' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is f881565d05338c4085d8f8a90f7882da.
Strike brokewell_0499377c	This strike sends a polymorphic malware sample known as Brokewell. Brokewell is an Android malware that is distributed via fake application updates. It masquerades as newer Chrome browser iterations or updates for an Austrian digital authentication application. Brokewell uses overlay attacks to capture user credentials and steals cookies by launching its own WebView and sending them to the command-and-control (C2) server. It captures every event happening on the device, including touches, swipes, displayed information, text input, and opened applications. 'zRFxj.ieubP.IWZZwlluca' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 0499377cef4de24a3d157c715b5c4123.

Name	Description
Strike brokewell_106322df	This strike sends a polymorphic malware sample known as Brokewell. Brokewell is an Android malware that is distributed via fake application updates. It masquerades as newer Chrome browser iterations or updates for an Austrian digital authentication application. Brokewell uses overlay attacks to capture user credentials and steals cookies by launching its own WebView and sending them to the command-and-control (C2) server. It captures every event happening on the device, including touches, swipes, displayed information, text input, and opened applications. 'zRFxj.ieubP.lWZzwlluca' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 106322df03c8bab33d712e968e59fb70.
Strike brokewell_4eb25733	This strike sends a malware sample known as Brokewell. Brokewell is an Android malware that is distributed via fake application updates. It masquerades as newer Chrome browser iterations or updates for an Austrian digital authentication application. Brokewell uses overlay attacks to capture user credentials and steals cookies by launching its own WebView and sending them to the command-and-control (C2) server. It captures every event happening on the device, including touches, swipes, displayed information, text input, and opened applications. 'jcwAz.EpLIq.vcAZiUGZpK' is the package name of the malware sample. The MD5 hash of this malware sample is 4eb2573387c0c1bb248cbfb0f1f8936f.
Strike brokewell_8932768d	This strike sends a malware sample known as Brokewell. Brokewell is an Android malware that is distributed via fake application updates. It masquerades as newer Chrome browser iterations or updates for an Austrian digital authentication application. Brokewell uses overlay attacks to capture user credentials and steals cookies by launching its own WebView and sending them to the command-and-control (C2) server. It captures every event happening on the device, including touches, swipes, displayed information, text input, and opened applications. 'zRFxj.ieubP.lWZzwlluca' is the package name of the malware sample. The MD5 hash of this malware sample is 8932768daaa490e27c7049ba772c8713.
Strike brokewell_a4fbffc5	This strike sends a polymorphic malware sample known as Brokewell. Brokewell is an Android malware that is distributed via fake application updates. It masquerades as newer Chrome browser iterations or updates for an Austrian digital authentication application. Brokewell uses overlay attacks to capture user credentials and steals cookies by launching its own WebView and sending them to the command-and-control (C2) server. It captures every event happening on the device, including touches, swipes, displayed information, text input, and opened applications. 'jcwAz.EpLIq.vcAZiUGZpK' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is a4fbffc5b88f93cab6ba4980300eb1be.

Name	Description
Strike brokewell_ddbf3a1d	This strike sends a polymorphic malware sample known as Brokewell. Brokewell is an Android malware that is distributed via fake application updates. It masquerades as newer Chrome browser iterations or updates for an Austrian digital authentication application. Brokewell uses overlay attacks to capture user credentials and steals cookies by launching its own WebView and sending them to the command-and-control (C2) server. It captures every event happening on the device, including touches, swipes, displayed information, text input, and opened applications. 'jcwAz.EpLIq.vcAZiUGZpK' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is ddbf3a1d8c4e0b097190cdd118275a4f.
Strike caprарат_021d8f6a	This strike sends a polymorphic malware sample known as CapraRAT. CapraRat is a spyware used by the group Transparent Tribe (APT 36). It disguises itself as video browsing apps targeting mobile gamers, weapons enthusiasts, and TikTok fans. CapraRat requests extensive permissions, such as GPS access, network state management, and SMS capabilities. Compared to previous campaigns, it focuses on surveillance rather than backdoor functionalities. The malware employs social engineering by mimicking legitimate apps like YouTube, embedding spyware into apps with preloaded queries related to popular themes, making it a persistent threat. 'com.maeps.crygms.tktols' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 021d8f6a4cc719f7137d78aaf459490f.
Strike caprарат_771a0946	This strike sends a polymorphic malware sample known as CapraRAT. CapraRat is a spyware used by the group Transparent Tribe (APT 36). It disguises itself as video browsing apps targeting mobile gamers, weapons enthusiasts, and TikTok fans. CapraRat requests extensive permissions, such as GPS access, network state management, and SMS capabilities. Compared to previous campaigns, it focuses on surveillance rather than backdoor functionalities. The malware employs social engineering by mimicking legitimate apps like YouTube, embedding spyware into apps with preloaded queries related to popular themes, making it a persistent threat. 'com.maeps.vdosa.tktols' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 771a0946aa53629d72f3bfdb211e9713.
Strike caprарат_91f2ba7f	This strike sends a malware sample known as CapraRAT. CapraRat is a spyware used by the group Transparent Tribe (APT 36). It disguises itself as video browsing apps targeting mobile gamers, weapons enthusiasts, and TikTok fans. CapraRat requests extensive permissions, such as GPS access, network state management, and SMS capabilities. Compared to previous campaigns, it focuses on surveillance rather than backdoor functionalities. The malware employs social engineering by mimicking legitimate apps like YouTube, embedding spyware into apps with preloaded queries related to popular themes, making it a persistent threat. 'com.maeps.vdosa.tktols' is the package name of the malware sample. The MD5 hash of this malware sample is 91f2ba7f9b327a694e92f06a4f0a0a7a.

<b>Name</b>	<b>Description</b>
Strike caprарат_a8d71b25	<p>This strike sends a polymorphic malware sample known as CapraRAT. CapraRat is a spyware used by the group Transparent Tribe (APT 36). It disguises itself as video browsing apps targeting mobile gamers, weapons enthusiasts, and TikTok fans. CapraRat requests extensive permissions, such as GPS access, network state management, and SMS capabilities. Compared to previous campaigns, it focuses on surveillance rather than backdoor functionalities. The malware employs social engineering by mimicking legitimate apps like YouTube, embedding spyware into apps with preloaded queries related to popular themes, making it a persistent threat. 'com.maeps.vdosa.tktols' is the package name of the malware sample. Constant strings in the code have been encrypted. The MD5 hash of this malware sample is a8d71b257d5fa97ea8dd5b8423552935.</p>
Strike caprарат_b6725d52	<p>This strike sends a polymorphic malware sample known as CapraRAT. CapraRat is a spyware used by the group Transparent Tribe (APT 36). It disguises itself as video browsing apps targeting mobile gamers, weapons enthusiasts, and TikTok fans. CapraRat requests extensive permissions, such as GPS access, network state management, and SMS capabilities. Compared to previous campaigns, it focuses on surveillance rather than backdoor functionalities. The malware employs social engineering by mimicking legitimate apps like YouTube, embedding spyware into apps with preloaded queries related to popular themes, making it a persistent threat. 'com.maeps.vdosa.tktols' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is b6725d5265d7634eaab48267aab38635.</p>
Strike caprарат_bd9dc9e0	<p>This strike sends a polymorphic malware sample known as CapraRAT. CapraRat is a spyware used by the group Transparent Tribe (APT 36). It disguises itself as video browsing apps targeting mobile gamers, weapons enthusiasts, and TikTok fans. CapraRat requests extensive permissions, such as GPS access, network state management, and SMS capabilities. Compared to previous campaigns, it focuses on surveillance rather than backdoor functionalities. The malware employs social engineering by mimicking legitimate apps like YouTube, embedding spyware into apps with preloaded queries related to popular themes, making it a persistent threat. 'com.maeps.crygms.tktols' is the package name of the malware sample. Constant strings in the code have been encrypted. The MD5 hash of this malware sample is bd9dc9e0d868a81c403ca486368a38e9.</p>
Strike caprарат_d104cc38	<p>This strike sends a polymorphic malware sample known as CapraRAT. CapraRat is a spyware used by the group Transparent Tribe (APT 36). It disguises itself as video browsing apps targeting mobile gamers, weapons enthusiasts, and TikTok fans. CapraRat requests extensive permissions, such as GPS access, network state management, and SMS capabilities. Compared to previous campaigns, it focuses on surveillance rather than backdoor functionalities. The malware employs social engineering by mimicking legitimate apps like YouTube, embedding spyware into apps with preloaded queries related to popular themes, making it a persistent threat. 'com.maeps.crygms.tktols' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is d104cc38073878ad301d3f507b5d7281.</p>

<b>Name</b>	<b>Description</b>
Strike caprарат_f2782f72	This strike sends a malware sample known as CapraRAT. CapraRat is a spyware used by the group Transparent Tribe (APT 36). It disguises itself as video browsing apps targeting mobile gamers, weapons enthusiasts, and TikTok fans. CapraRat requests extensive permissions, such as GPS access, network state management, and SMS capabilities. Compared to previous campaigns, it focuses on surveillance rather than backdoor functionalities. The malware employs social engineering by mimicking legitimate apps like YouTube, embedding spyware into apps with preloaded queries related to popular themes, making it a persistent threat. 'com.maeps.crygms.tktols' is the package name of the malware sample. The MD5 hash of this malware sample is f2782f72ecf124642777a89d36195d55.
Strike dcRAT_033ee7d8	This strike sends a polymorphic malware sample known as dcRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is dcRAT. The binary has the timestamp field updated in the PE file header. The MD5 hash of this dcRAT sample is 033ee7d8c8e304c5925d551f6c12b665.
Strike dcRAT_37255857	This strike sends a malware sample known as dcRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is dcRAT. The MD5 hash of this dcRAT sample is 37255857bd1fc48c7fcc2a3fa8af86a5.
Strike dcRAT_46614cb5	This strike sends a polymorphic malware sample known as dcRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is dcRAT. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this dcRAT sample is 46614cb5a9fd99be0b24f4b094698aef.
Strike dcRAT_757005d3	This strike sends a malware sample known as dcRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is dcRAT. The MD5 hash of this dcRAT sample is 757005d3bb12ce3f9146d8027b236c9b.
Strike dcRAT_915b0fbb	This strike sends a polymorphic malware sample known as dcRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is dcRAT. The binary has random bytes appended at the end of the file. The MD5 hash of this dcRAT sample is 915b0fbb556fe6f8a48c3f5da0cb28ec.

<b>Name</b>	<b>Description</b>
Strike dcRAT_a982d253	This strike sends a polymorphic malware sample known as dcRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is dcRAT. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this dcRAT sample is a982d253aad5976b951ecb1a48933fde.
Strike dcRAT_f3c91609	This strike sends a polymorphic malware sample known as dcRAT. In Oct 2021 Cisco Talos detected a campaign targeting Afghanistan and India utilizing malicious RTF documents to deliver malware to its victims. This campaign used CVE-2017-11882, a vulnerability in Microsoft Office, to deliver QuasarRAT and dcRAT to Windows and AndroidRAT to mobile devices. This sample is dcRAT. The binary has a new section added in the PE file format with random contents. The MD5 hash of this dcRAT sample is f3c91609bffe4ac5814a5bf0324467bd.
Strike donot_13f3862b	This strike sends a polymorphic malware sample associated with the DoNot APT group. The group utilizes an open-source project from GitHub, augmenting it with malicious code for weaponization. This malware introduces enhanced functionalities, including the ability to record VoIP calls from messaging applications, capturing clipboard contents, downloading payloads dynamically, collecting browser history, and gathering other forms of Personally Identifiable Information (PII) data and ShareMe activity. The malware employs the Firebase Cloud Messaging (FCM) server as its initial Command and Control (C2) server, managing various functions, including obtaining new C2 server URLs, configuring databases, uninstalling the application, sending text messages, adding contacts, logging calls, and downloading APK files. 'com.syster.serviceapp' is the package name of the malware sample. Constant strings in the code of the malware have been encrypted. The MD5 hash of this malware sample is 13f3862bce2b20b7e2a8aa39b18eab3d.
Strike donot_14302b21	This strike sends a polymorphic malware sample associated with the DoNot APT group. The group utilizes an open-source project from GitHub, augmenting it with malicious code for weaponization. This malware introduces enhanced functionalities, including the ability to record VoIP calls from messaging applications, capturing clipboard contents, downloading payloads dynamically, collecting browser history, and gathering other forms of Personally Identifiable Information (PII) data and ShareMe activity. The malware employs the Firebase Cloud Messaging (FCM) server as its initial Command and Control (C2) server, managing various functions, including obtaining new C2 server URLs, configuring databases, uninstalling the application, sending text messages, adding contacts, logging calls, and downloading APK files. 'com.syster.serviceapp' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 14302b218060aac3e9ee23d09feffb.

<b>Name</b>	<b>Description</b>
Strike donot_1445e89f	<p>This strike sends a malware sample associated with the DoNot APT group. The group utilizes an open-source project from GitHub, augmenting it with malicious code for weaponization. This malware introduces enhanced functionalities, including the ability to record VoIP calls from messaging applications, capturing clipboard contents, downloading payloads dynamically, collecting browser history, and gathering other forms of Personally Identifiable Information (PII) data and ShareMe activity. The malware employs the Firebase Cloud Messaging (FCM) server as its initial Command and Control (C2) server, managing various functions, including obtaining new C2 server URLs, configuring databases, uninstalling the application, sending text messages, adding contacts, logging calls, and downloading APK files. 'com.syster.serviceapp' is the package name of the malware sample. The MD5 hash of this malware sample is 1445e89f793c6f9881ce11432fe8a3ce.</p>
Strike donot_22043936	<p>This strike sends a polymorphic malware sample associated with the DoNot APT group. The group utilizes an open-source project from GitHub, augmenting it with malicious code for weaponization. This malware introduces enhanced functionalities, including the ability to record VoIP calls from messaging applications, capturing clipboard contents, downloading payloads dynamically, collecting browser history, and gathering other forms of Personally Identifiable Information (PII) data and ShareMe activity. The malware employs the Firebase Cloud Messaging (FCM) server as its initial Command and Control (C2) server, managing various functions, including obtaining new C2 server URLs, configuring databases, uninstalling the application, sending text messages, adding contacts, logging calls, and downloading APK files. 'com.syster.serviceapp' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 22043936d5b59339d628aaaf54d42c996.</p>
Strike eXoticVisit_15f2f960	<p>This strike sends a polymorphic malware sample known as eXotic Visit. It belongs to the espionage campaign named eXotic Visit, targeting Android users in South Asia. It is distributed through dedicated websites and via the Google Play Store, often bundled with the open-source XploitSpy malware. The malware masquerades as a legitimate messaging application and is capable of extracting contact lists and files from the device. Additionally, it can obtain the device's GPS location and access filenames related to camera, downloads, and messaging apps. It executes additional commands from the C2 server to extract specific files of interest. 'com.tech.sideswipechat' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 15f2f960bc0218b782f8d76df3d0dc8a.</p>
Strike eXoticVisit_1910399f	<p>This strike sends a polymorphic malware sample known as eXotic Visit. It belongs to the espionage campaign named eXotic Visit, targeting Android users in South Asia. It is distributed through dedicated websites and via the Google Play Store, often bundled with the open-source XploitSpy malware. The malware masquerades as a legitimate messaging application and is capable of extracting contact lists and files from the device. Additionally, it can obtain the device's GPS location and access filenames related to camera, downloads, and messaging apps. It executes additional commands from the C2 server to extract specific files of interest. 'com.developerup.chatapp' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 1910399f35c65dc156afe73e0e90ce1b.</p>

<b>Name</b>	<b>Description</b>
Strike eXoticVisit_1f82b889	<p>This strike sends a polymorphic malware sample known as eXotic Visit. It belongs to the espionage campaign named eXotic Visit, targeting Android users in South Asia. It is distributed through dedicated websites and via the Google Play Store, often bundled with the open-source XploitSpy malware. The malware masquerades as a legitimate messaging application and is capable of extracting contact lists and files from the device. Additionally, it can obtain the device's GPS location and access filenames related to camera, downloads, and messaging apps. It executes additional commands from the C2 server to extract specific files of interest.</p> <p>'com.egoosoft.siminfo' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 1f82b889c036127ba2f6126221b15ebb.</p>
Strike eXoticVisit_402fcfa0	<p>This strike sends a polymorphic malware sample known as eXotic Visit. It belongs to the espionage campaign named eXotic Visit, targeting Android users in South Asia. It is distributed through dedicated websites and via the Google Play Store, often bundled with the open-source XploitSpy malware. The malware masquerades as a legitimate messaging application and is capable of extracting contact lists and files from the device. Additionally, it can obtain the device's GPS location and access filenames related to camera, downloads, and messaging apps. It executes additional commands from the C2 server to extract specific files of interest.</p> <p>'com.tech.sideswipechat' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 402fcfa0a50f0181f74d1d00098b0d58.</p>
Strike eXoticVisit_49146d2e	<p>This strike sends a polymorphic malware sample known as eXotic Visit. It belongs to the espionage campaign named eXotic Visit, targeting Android users in South Asia. It is distributed through dedicated websites and via the Google Play Store, often bundled with the open-source XploitSpy malware. The malware masquerades as a legitimate messaging application and is capable of extracting contact lists and files from the device. Additionally, it can obtain the device's GPS location and access filenames related to camera, downloads, and messaging apps. It executes additional commands from the C2 server to extract specific files of interest.</p> <p>'com.developerup.chatapp' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 49146d2e88fefdeb0ac6b1f4f76ee658.</p>
Strike eXoticVisit_4dd159ff	<p>This strike sends a malware sample known as eXotic Visit. It belongs to the espionage campaign named eXotic Visit, targeting Android users in South Asia. It is distributed through dedicated websites and via the Google Play Store, often bundled with the open-source XploitSpy malware. The malware masquerades as a legitimate messaging application and is capable of extracting contact lists and files from the device. Additionally, it can obtain the device's GPS location and access filenames related to camera, downloads, and messaging apps. It executes additional commands from the C2 server to extract specific files of interest. 'com.egoosoft.siminfo' is the package name of the malware sample. The MD5 hash of this malware sample is 4dd159ff4243d02dd43043860af9691f.</p>

<b>Name</b>	<b>Description</b>
Strike eXoticVisit_62ffe765	<p>This strike sends a polymorphic malware sample known as eXotic Visit. It belongs to the espionage campaign named eXotic Visit, targeting Android users in South Asia. It is distributed through dedicated websites and via the Google Play Store, often bundled with the open-source XploitSpy malware. The malware masquerades as a legitimate messaging application and is capable of extracting contact lists and files from the device. Additionally, it can obtain the device's GPS location and access filenames related to camera, downloads, and messaging apps. It executes additional commands from the C2 server to extract specific files of interest.</p> <p>'com.egoosoft.siminfo' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 62ffe7651146dd496f382cc437ee9070.</p>
Strike eXoticVisit_d73c267b	<p>This strike sends a polymorphic malware sample known as eXotic Visit. It belongs to the espionage campaign named eXotic Visit, targeting Android users in South Asia. It is distributed through dedicated websites and via the Google Play Store, often bundled with the open-source XploitSpy malware. The malware masquerades as a legitimate messaging application and is capable of extracting contact lists and files from the device. Additionally, it can obtain the device's GPS location and access filenames related to camera, downloads, and messaging apps. It executes additional commands from the C2 server to extract specific files of interest.</p> <p>'com.egoosoft.siminfo' is the package name of the malware sample. Constant strings in the code have been encrypted. The MD5 hash of this malware sample is d73c267b5c13f1b39e963521aa064c5d.</p>
Strike eXoticVisit_deba43a7	<p>This strike sends a malware sample known as eXotic Visit. It belongs to the espionage campaign named eXotic Visit, targeting Android users in South Asia. It is distributed through dedicated websites and via the Google Play Store, often bundled with the open-source XploitSpy malware. The malware masquerades as a legitimate messaging application and is capable of extracting contact lists and files from the device. Additionally, it can obtain the device's GPS location and access filenames related to camera, downloads, and messaging apps. It executes additional commands from the C2 server to extract specific files of interest. 'com.tech.sideswipechat' is the package name of the malware sample. The MD5 hash of this malware sample is deba43a71712c3a501970e3fc5ab1ced.</p>
Strike eXoticVisit_e5a3a1b3	<p>This strike sends a malware sample known as eXotic Visit. It belongs to the espionage campaign named eXotic Visit, targeting Android users in South Asia. It is distributed through dedicated websites and via the Google Play Store, often bundled with the open-source XploitSpy malware. The malware masquerades as a legitimate messaging application and is capable of extracting contact lists and files from the device. Additionally, it can obtain the device's GPS location and access filenames related to camera, downloads, and messaging apps. It executes additional commands from the C2 server to extract specific files of interest. 'com.developerup.chatapp' is the package name of the malware sample. The MD5 hash of this malware sample is e5a3a1b379fa3d861aa5518e34c54e6a.</p>

<b>Name</b>	<b>Description</b>
Strike hiddenad_2199cc1d	This strike sends a polymorphic malware sample known as HiddenAd. HiddenAd is a type of adware that aggressively displays unwanted advertisements to Android users, generating revenue for its creators. This malware disguises itself as benign Android applications to hide its true purpose. It hides its application icon, encrypts its critical payloads in an SQLCipher database, and employs obfuscation techniques to evade detection. Its primary goal is to bombard users with ads and potentially lead to other security threats on Android devices. 'mapa.com' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 2199cc1db5c9fb1865f1df188977a08a.
Strike hiddenad_baa63680	This strike sends a malware sample known as HiddenAd. HiddenAd is a type of adware that aggressively displays unwanted advertisements to Android users, generating revenue for its creators. This malware disguises itself as benign Android applications to hide its true purpose. It hides its application icon, encrypts its critical payloads in an SQLCipher database, and employs obfuscation techniques to evade detection. Its primary goal is to bombard users with ads and potentially lead to other security threats on Android devices. 'mapa.com' is the package name of the malware sample. The MD5 hash of this malware sample is baa63680fb9c11c6675e01242fe6d920.
Strike hiddenad_df520950	This strike sends a polymorphic malware sample known as HiddenAd. HiddenAd is a type of adware that aggressively displays unwanted advertisements to Android users, generating revenue for its creators. This malware disguises itself as benign Android applications to hide its true purpose. It hides its application icon, encrypts its critical payloads in an SQLCipher database, and employs obfuscation techniques to evade detection. Its primary goal is to bombard users with ads and potentially lead to other security threats on Android devices. 'mapa.com' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is df520950a2817e512d6e28ef95769800.
Strike kill-floor_40439f39	This strike sends a malware sample known as kill-floor. kill-floor malware is a kernel level rootkit malware that has been detected in the wild taking advantage of a legitimate anti-rootkit driver in order to bypass native security mechanisms in order to infect the system. This Bring Your Own Vulnerable Driver malware drops a legitimate Avast Anti-Rootkit driver to gain kernel-level access to the system and terminate security processes. Once the driver is installed it creates a service that begins logging running processes on the system. It uses this information to compare against known software and begins terminating the software that it matches. The MD5 hash of this kill-floor sample is 40439f39f0195c9c7a3b519554afd17a.
Strike llm_enabled_1854a442	This strike sends a malware sample known as llm_enabled. LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this llm_enabled sample is 1854a4427eef0f74d16ad555617775ff.

<b>Name</b>	<b>Description</b>
Strike llm_enabled_1952345e	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>1952345e66e1f3173190d282f810a37d</code> .
Strike llm_enabled_1a6be50d	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>1a6be50d9839d2e4dcd6b028df05b334</code> .
Strike llm_enabled_2fdffdf0	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>2fdffdf0b099cc195316a85636e9636d</code> .
Strike llm_enabled_40b179e3	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>40b179e334fd12241823e4ad353bb96d</code> .
Strike llm_enabled_651d69c8	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>651d69c843f827f9ed871f595ffa15e5</code> .

<b>Name</b>	<b>Description</b>
Strike llm_enabled_74eb831b	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>74eb831b26a21d954261658c72145128</code> .
Strike llm_enabled_806f5520	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>806f552041f211a35e434112a0165568</code> .
Strike llm_enabled_81cd2031	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>81cd20319c8f0b2ce499f9253ce0a6a8</code> .
Strike llm_enabled_9d92b543	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>9d92b5436a0e75471de4b583696b33ac</code> .
Strike llm_enabled_ac377e26	This strike sends a malware sample known as <code>llm_enabled</code> . LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this <code>llm_enabled</code> sample is <code>ac377e26c24f50b4d9aaa933d788c18c</code> .

Name	Description
Strike llm_enabled_ed229f34	This strike sends a malware sample known as llm_enabled. LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this llm_enabled sample is ed229f3442f2d45f6fdd4f3a4c552c1c.
Strike llm_enabled_f7cf07f2	This strike sends a malware sample known as llm_enabled. LLM-enabled malware is a type of malware that uses Living-off-the-Land (LotL) binaries and scripts to infiltrate and compromise systems. It is delivered through malicious documents, often embedded with macros, that prompt users to enable editing or content. Once executed, the malware uses embedded scripts to download and execute additional payloads from a remote server. Its key capabilities include evading detection by using legitimate system tools, establishing persistence, and downloading and executing additional malicious payloads. The MD5 hash of this llm_enabled sample is f7cf07f2bf07fcf054ac909d8ae6223d.
Strike mandrake_01897090	This strike sends a polymorphic malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, demonstrating its evolving nature to evade detection and infiltrate official app marketplaces. 'com.cryptopulsing.browser' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 01897090a54d790c8626e4fa4c8bb9e1.
Strike mandrake_03fec806	This strike sends a polymorphic malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, demonstrating its evolving nature to evade detection and infiltrate official app marketplaces. 'com.cryptopulsing.browser' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 03fec806232bf085930c7a19a5a2a78b.

Name	Description
Strike mandrake_5a41f9d1	This strike sends a polymorphic malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, demonstrating its evolving nature to evade detection and infiltrate official app marketplaces. 'com.cryptopulsing.browser' is the package name of the malware sample. Constant strings in the code has been encrypted. The MD5 hash of this malware sample is 5a41f9d10df6fdfde29b66e9fdf4336e.
Strike mandrake_e165cda2	This strike sends a malware sample known as Mandrake. Mandrake is a sophisticated malware that operates in multiple stages, starting with a dropper that downloads the payload from a command-and-control (C2) server. It collects detailed device information, including installed apps and external IP, and requests permissions to run in the background. In its final stage, Mandrake steals user credentials by loading URLs, initiating remote screen-sharing sessions, and recording the device's screen. It bypasses Android 13 security features using a session-based installer, demonstrating its evolving nature to evade detection and infiltrate official app marketplaces. 'com.cryptopulsing.browser' is the package name of the malware sample. The MD5 hash of this malware sample is e165cda25ef49c02ed94ab524fafa938.
Strike moonshine_03b0d0b2	This strike sends a polymorphic polymorphic malware sample known as Moonshine. MOONSHINE is an Android malware that targets vulnerabilities in instant messaging apps, primarily affecting Tibetan and Uyghur communities. It infects devices with a cross-platform backdoor named DarkNimbus. The malware employs social engineering techniques to lure victims into clicking malicious links which downloads the backdoor. 'com.android.asys' is the package name of the malware sample. Constant strings in the code has been encrypted. The MD5 hash of this malware sample is 03b0d0b2002c89dfd479032c008e70bd.
Strike moonshine_079c14eb	This strike sends a polymorphic malware sample known as Moonshine. MOONSHINE is an Android malware that targets vulnerabilities in instant messaging apps, primarily affecting Tibetan and Uyghur communities. It infects devices with a cross-platform backdoor named DarkNimbus. The malware employs social engineering techniques to lure victims into clicking malicious links which downloads the backdoor. 'com.android.asys' is the package name of the malware sample. The MD5 hash of this malware sample is 079c14eb237a32c2d7897e46a22fff7e.
Strike moonshine_19677682	This strike sends a polymorphic polymorphic malware sample known as Moonshine. MOONSHINE is an Android malware that targets vulnerabilities in instant messaging apps, primarily affecting Tibetan and Uyghur communities. It infects devices with a cross-platform backdoor named DarkNimbus. The malware employs social engineering techniques to lure victims into clicking malicious links which downloads the backdoor. 'com.android.asys' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 1967768217c4fa5cd799225f2fa052bd.

<b>Name</b>	<b>Description</b>
Strike moonshine_5911dfa9	This strike sends a polymorphic polymorphic malware sample known as Moonshine. MOONSHINE is an Android malware that targets vulnerabilities in instant messaging apps, primarily affecting Tibetan and Uyghur communities. It infects devices with a cross-platform backdoor named DarkNimbus. The malware employs social engineering techniques to lure victims into clicking malicious links which downloads the backdoor. 'com.android.asys' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 5911dfa951864fbb8996f3c45fbb8f56.
Strike moonshine_7aa95b1a	This strike sends a polymorphic polymorphic malware sample known as Moonshine. MOONSHINE is an Android malware that targets vulnerabilities in instant messaging apps, primarily affecting Tibetan and Uyghur communities. It infects devices with a cross-platform backdoor named DarkNimbus. The malware employs social engineering techniques to lure victims into clicking malicious links which downloads the backdoor. 'com.android.asys' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 7aa95b1a00099c590672297a21a4ecc5.
Strike moonshine_9c6f0178	This strike sends a polymorphic malware sample known as Moonshine. MOONSHINE is an Android malware that targets vulnerabilities in instant messaging apps, primarily affecting Tibetan and Uyghur communities. It infects devices with a cross-platform backdoor named DarkNimbus. The malware employs social engineering techniques to lure victims into clicking malicious links which downloads the backdoor. 'com.android.asys' is the package name of the malware sample. The MD5 hash of this malware sample is 9c6f0178cec7ac5036803ce3e569c901.
Strike moonshine_bba2a24a	This strike sends a polymorphic polymorphic malware sample known as Moonshine. MOONSHINE is an Android malware that targets vulnerabilities in instant messaging apps, primarily affecting Tibetan and Uyghur communities. It infects devices with a cross-platform backdoor named DarkNimbus. The malware employs social engineering techniques to lure victims into clicking malicious links which downloads the backdoor. 'com.android.asys' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is bba2a24a740b88cb812f0799e232374e.
Strike napchat_23955a9a	This strike sends a polymorphic malware sample known as NapChat App 1.0.apk, associated with the DoNot APT group. The group utilizes an open-source project from GitHub, augmenting it with malicious code for weaponization. This malware introduces enhanced functionalities, including the ability to record VoIP calls, collect messages from messaging and social media apps, and gather diverse data types. The malware employs an advanced command and control structure, utilizing a Firebase Cloud Messaging (FCM) server alongside two auxiliary command and control servers for communication. The stolen data is systematically stored in an SQLite database. 'com.jio.join' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 23955a9af742bfe4f115db819dc44f99.

Name	Description
Strike napchat_26850d7b	This strike sends a malware sample known as NapChat App 1.0.apk, associated with the DoNot APT group. The group utilizes an open-source project from GitHub, augmenting it with malicious code for weaponization. This malware introduces enhanced functionalities, including the ability to record VoIP calls, collect messages from messaging and social media apps, and gather diverse data types. The malware employs an advanced command and control structure, utilizing a Firebase Cloud Messaging (FCM) server alongside two auxiliary command and control servers for communication. The stolen data is systematically stored in an SQLite database. 'com.jio.join' is the package name of the malware sample. The MD5 hash of this malware sample is 26850d7b5e900b2e00c8c610c1294a78.
Strike napchat_737a07be	This strike sends a polymorphic malware sample known as NapChat App 1.0.apk, associated with the DoNot APT group. The group utilizes an open-source project from GitHub, augmenting it with malicious code for weaponization. This malware introduces enhanced functionalities, including the ability to record VoIP calls, collect messages from messaging and social media apps, and gather diverse data types. The malware employs an advanced command and control structure, utilizing a Firebase Cloud Messaging (FCM) server alongside two auxiliary command and control servers for communication. The stolen data is systematically stored in an SQLite database. 'com.jio.join' is the package name of the malware sample. Constant strings in the code of the malware have been encrypted. The MD5 hash of this malware sample is 737a07be6b7b3eca7e2f7aaa9951a9f8.
Strike necro_1e0aa099	This strike sends a polymorphic malware sample known as Necro. Necro is a sophisticated multi-stage loader that downloads and executes malicious payloads. It uses techniques like steganography and obfuscation to evade detection. Once a device is infected, is capable of dynamically loading modules that perform various malicious activities, like installing apps, clicking on ads in the background without user interaction and subscribing users to paid services. It periodically contacts a C2 server to execute arbitrary code with elevated permissions and load specific links. 'com.omg.owner' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 1e0aa099a739b93a40a9d9f54c3218c4.
Strike necro_1eaf43be	This strike sends a malware sample known as Necro. Necro is a sophisticated multi-stage loader that downloads and executes malicious payloads. It uses techniques like steganography and obfuscation to evade detection. Once a device is infected, is capable of dynamically loading modules that perform various malicious activities, like installing apps, clicking on ads in the background without user interaction and subscribing users to paid services. It periodically contacts a C2 server to execute arbitrary code with elevated permissions and load specific links. 'com.omg.owner' is the package name of the malware sample. The MD5 hash of this malware sample is 1eaf43be379927e050126e5a7287eb98.

<b>Name</b>	<b>Description</b>
Strike necro_b359f4c9	<p>This strike sends a polymorphic malware sample known as Necro. Necro is a sophisticated multi-stage loader that downloads and executes malicious payloads. It uses techniques like steganography and obfuscation to evade detection. Once a device is infected, it is capable of dynamically loading modules that perform various malicious activities, like installing apps, clicking on ads in the background without user interaction and subscribing users to paid services. It periodically contacts a C2 server to execute arbitrary code with elevated permissions and load specific links.</p> <p>'com.omg.ownner' is the package name of the malware sample. Constant strings in the code have been encrypted. The MD5 hash of this malware sample is b359f4c9c8a8883c7d43a277fe8735ea.</p>
Strike necro_e1b9826e	<p>This strike sends a polymorphic malware sample known as Necro. Necro is a sophisticated multi-stage loader that downloads and executes malicious payloads. It uses techniques like steganography and obfuscation to evade detection. Once a device is infected, it is capable of dynamically loading modules that perform various malicious activities, like installing apps, clicking on ads in the background without user interaction and subscribing users to paid services. It periodically contacts a C2 server to execute arbitrary code with elevated permissions and load specific links.</p> <p>'com.omg.ownner' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is e1b9826e4d1c0c638842b7ec3caa5211.</p>
Strike ngate_336a7d94	<p>This strike sends a polymorphic malware sample known as NGate. The malware operates by exploiting the Near Field Communication (NFC) chip in Android devices to read and capture credit card details from contactless payment cards that are in close proximity to the infected device. It spreads through phishing techniques and is capable of capturing, relaying, replaying, and cloning data on the infected device. 'rb.system.com' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 336a7d9420fcb538f169081bc0597b50.</p>
Strike ngate_5b971c7c	<p>This strike sends a polymorphic malware sample known as NGate. The malware operates by exploiting the Near Field Communication (NFC) chip in Android devices to read and capture credit card details from contactless payment cards that are in close proximity to the infected device. It spreads through phishing techniques and is capable of capturing, relaying, replaying, and cloning data on the infected device. 'rb.system.com' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 5b971c7cf15acc7f9f72dc3238d916b4.</p>
Strike ngate_76bc1612	<p>This strike sends a polymorphic malware sample known as NGate. The malware operates by exploiting the Near Field Communication (NFC) chip in Android devices to read and capture credit card details from contactless payment cards that are in close proximity to the infected device. It spreads through phishing techniques and is capable of capturing, relaying, replaying, and cloning data on the infected device. 'rb.system.com' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 76bc16122f8ca654ad0096eb7bddcff5.</p>

<b>Name</b>	<b>Description</b>
Strike ngate_8595855e	This strike sends a malware sample known as NGate. The malware operates by exploiting the Near Field Communication (NFC) chip in Android devices to read and capture credit card details from contactless payment cards that are in close proximity to the infected device. It spreads through phishing techniques and is capable of capturing, relaying, replaying, and cloning data on the infected device. 'rb.system.com' is the package name of the malware sample. The MD5 hash of this malware sample is 8595855eaf9fe0398c8bff7fa06151bf.
Strike ngate_d346be46	This strike sends a polymorphic malware sample known as NGate. The malware operates by exploiting the Near Field Communication (NFC) chip in Android devices to read and capture credit card details from contactless payment cards that are in close proximity to the infected device. It spreads through phishing techniques and is capable of capturing, relaying, replaying, and cloning data on the infected device. 'rb.system.com' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is d346be464800b74f9ec744356624ec1f.
Strike ngate_ea6a6666	This strike sends a malware sample known as NGate. The malware operates by exploiting the Near Field Communication (NFC) chip in Android devices to read and capture credit card details from contactless payment cards that are in close proximity to the infected device. It spreads through phishing techniques and is capable of capturing, relaying, replaying, and cloning data on the infected device. 'rb.system.com' is the package name of the malware sample. The MD5 hash of this malware sample is ea6a6666616f6b02c7b679782a676eab.
Strike nimbus_manticore_14d8e865	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is 14d8e865d3ca67b88c01f7e5d2b0862d.
Strike nimbus_manticore_3a85381d	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is 3a85381dd880c69f40b02859cd9fd473.
Strike nimbus_manticore_77667725	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is 776677256087a5a0f543a6b6317cadf8.

<b>Name</b>	<b>Description</b>
Strike nimbus_manticore_83b7ec5f	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is 83b7ec5f0d5d6f11ba1284a3f705e98e.
Strike nimbus_manticore_96a9078d	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is 96a9078d97a8b2a0cdc6632b48b8a649.
Strike nimbus_manticore_b40533e6	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is b40533e67e70b7ff7bb53d34a4b9170e.
Strike nimbus_manticore_b7e4b752	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is b7e4b752adff07ac1b7b67a9be30b366.
Strike nimbus_manticore_be2bd408	This strike sends a malware sample known as nimbus_manticore. Nimbus Manticore is a malware that functions as a banking Trojan and targets European countries. It is distributed through malicious email attachments and exploits vulnerabilities in Microsoft Office and Adobe Acrobat Reader. Once executed, the malware downloads and installs additional malicious payloads, including ransomware and banking Trojans. Its key capabilities include disabling antivirus software, stealing financial information, and encrypting user files for ransom. The MD5 hash of this nimbus_manticore sample is be2bd408c615997c600871970573f023.
Strike njRAT_05ab3ea1	This strike sends a malware sample known as njRAT. njRAT, also known as Bladabindi, is a remote access trojan (RAT) that allows attackers to execute commands on the infected host, log keystrokes, and remotely turn on the victim's webcam and microphone. njRAT was developed by the Sparclyheason group. Some of the largest attacks using this malware date back to 2014. These samples were detected in a campaign that abused Microsoft's Dev Tunnels service for C2 communication. The MD5 hash of this njRAT sample is 05ab3ea12a0be22475e21c60242ce4a1.

<b>Name</b>	<b>Description</b>
Strike njRAT_12b18de1	This strike sends a malware sample known as njRAT. This malicious sample known as njRAT is also known as Bladabindi. It is a remote access trojan (RAT) that allows attackers to execute commands on the infected host, log keystrokes and remotely turn on the victim's webcam and microphone. njRAT was developed by the Sparclyheason group. Some of the largest attacks using this malware date back to 2014. The MD5 hash of this njRAT sample is 12b18de18774e20d12108675ae703cd1.
Strike njRAT_4e761f5c	This strike sends a malware sample known as njRAT. This malicious sample known as njRAT is also known as Bladabindi. It is a remote access trojan (RAT) that allows attackers to execute commands on the infected host, log keystrokes and remotely turn on the victim's webcam and microphone. njRAT was developed by the Sparclyheason group. Some of the largest attacks using this malware date back to 2014. The MD5 hash of this njRAT sample is 4e761f5c94c5c4edf56693ad5b41f570.
Strike njRAT_5eb2f727	This strike sends a malware sample known as njRAT. This malicious sample known as njRAT is also known as Bladabindi. It is a remote access trojan (RAT) that allows attackers to execute commands on the infected host, log keystrokes and remotely turn on the victim's webcam and microphone. njRAT was developed by the Sparclyheason group. Some of the largest attacks using this malware date back to 2014. The MD5 hash of this njRAT sample is 5eb2f7278d921c82d361c299acfe4b9b.
Strike njRAT_8651b7ab	This strike sends a malware sample known as njRAT. This malicious sample known as njRAT is also known as Bladabindi. It is a remote access trojan (RAT) that allows attackers to execute commands on the infected host, log keystrokes and remotely turn on the victim's webcam and microphone. njRAT was developed by the Sparclyheason group. Some of the largest attacks using this malware date back to 2014. The MD5 hash of this njRAT sample is 8651b7abaaf04ef05955dd420a3acf4f.
Strike njRAT_905e94b4	This strike sends a malware sample known as njRAT. This malicious sample known as njRAT is also known as Bladabindi. It is a remote access trojan (RAT) that allows attackers to execute commands on the infected host, log keystrokes and remotely turn on the victim's webcam and microphone. njRAT was developed by the Sparclyheason group. Some of the largest attacks using this malware date back to 2014. The MD5 hash of this njRAT sample is 905e94b434090c293e959abad892f7f6.
Strike njRAT_96903e1d	This strike sends a malware sample known as njRAT. njRAT, also known as Bladabindi, is a remote access trojan (RAT) that allows attackers to execute commands on the infected host, log keystrokes, and remotely turn on the victim's webcam and microphone. njRAT was developed by the Sparclyheason group. Some of the largest attacks using this malware date back to 2014. These samples were detected in a campaign that abused Microsoft's Dev Tunnels service for C2 communication. The MD5 hash of this njRAT sample is 96903e1d3c6f9ac5bd32701a063197ae.
Strike njRAT_cf7a5bee	This strike sends a malware sample known as njRAT. This malicious sample known as njRAT is also known as Bladabindi. It is a remote access trojan (RAT) that allows attackers to execute commands on the infected host, log keystrokes and remotely turn on the victim's webcam and microphone. njRAT was developed by the Sparclyheason group. Some of the largest attacks using this malware date back to 2014. The MD5 hash of this njRAT sample is cf7a5beeff4812e7133265ae7d13628a.

<b>Name</b>	<b>Description</b>
Strike njRAT_d83a17e6	This strike sends a malware sample known as njRAT. This malicious sample known as njRAT is also known as Bladabindi. It is a remote access trojan (RAT) that allows attackers to execute commands on the infected host, log keystrokes and remotely turn on the victim's webcam and microphone. njRAT was developed by the Sparclyheason group. Some of the largest attacks using this malware date back to 2014. The MD5 hash of this njRAT sample is d83a17e6ba176d0dbbdf0b81ec063aba.
Strike njRAT_e3dc900c	This strike sends a malware sample known as njRAT. This malicious sample known as njRAT is also known as Bladabindi. It is a remote access trojan (RAT) that allows attackers to execute commands on the infected host, log keystrokes and remotely turn on the victim's webcam and microphone. njRAT was developed by the Sparclyheason group. Some of the largest attacks using this malware date back to 2014. The MD5 hash of this njRAT sample is e3dc900cceaa448b432e1b1662b3fd36d.
Strike njRAT_ec7c3988	This strike sends a malware sample known as njRAT. This malicious sample known as njRAT is also known as Bladabindi. It is a remote access trojan (RAT) that allows attackers to execute commands on the infected host, log keystrokes and remotely turn on the victim's webcam and microphone. njRAT was developed by the Sparclyheason group. Some of the largest attacks using this malware date back to 2014. The MD5 hash of this njRAT sample is ec7c39883859e7b2a4ba7ecce9011d04.
Strike operation_rewrite_0721efb9	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 0721efb9a3e364a372bbb4b7b7c42193.
Strike operation_rewrite_5ed7d3f4	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 5ed7d3f4e83c9456363c0502a7b00fac.

<b>Name</b>	<b>Description</b>
Strike operation_rewrite_6049f6d2	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 6049f6d24d84b335ae8eb19d049e9e42.
Strike operation_rewrite_6cada79f	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 6cada79fd399172f4ff55774ad1954ce.
Strike operation_rewrite_728605f7	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 728605f7586642a814e900e9b2f236fb.
Strike operation_rewrite_74863e3 5	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 74863e35f68f27386eb0f65528b5855a.
Strike operation_rewrite_920a193 8	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 920a193888df5adef270d3f05e907d8b.

<b>Name</b>	<b>Description</b>
Strike operation_rewrite_941cf054	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 941cf0549f9246c655e77767cacb8666.
Strike operation_rewrite_97a7823 8	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is 97a78238ffa97e140d05d18611979d55.
Strike operation_rewrite_a98432ed	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is a98432ed45af026f93fb450fd9ebcdda.
Strike operation_rewrite_b1760f43	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is b1760f43574b88382fcfdc589ca458254.
Strike operation_rewrite_db3652d 4	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is db3652d42598323481d3168409b5b9bb.

<b>Name</b>	<b>Description</b>
Strike operation_rewrite_e50a3e80	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is e50a3e8071e49e17d4d11e98e57cddc8.
Strike operation_rewrite_e7e8240b	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is e7e8240be190f80c52fd4c8f26f61f68.
Strike operation_rewrite_eb84dc41	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is eb84dc4121511343b0336c92715cbe5.
Strike operation_rewrite_ebe4e970	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is ebe4e97053230d841d9f5fca62caf9ac.
Strike operation_rewrite_f4136470	This strike sends a malware sample known as operation_rewrite. Operation Rewrite is a malware campaign that involves SEO poisoning and redirection to malicious websites. The threat actors use blackhat SEO techniques, including the creation of spam pages and the manipulation of search engine algorithms, to drive traffic to their websites. When a user visits these websites, they are redirected to malicious sites that either host phishing pages or exploit kits. The key capabilities of this malware campaign include website redirection, SEO manipulation, and the potential to deliver further malware through exploit kits or phishing attacks. The MD5 hash of this operation_rewrite sample is f413647083a0701e91b5a2fc247fd586.

<b>Name</b>	<b>Description</b>
Strike rafelrat_16c6c99d	<p>This strike sends a polymorphic malware sample known as Rafel RAT. Rafel RAT is a sophisticated Android malware that has evolved from espionage to ransomware operations. It is transmitted through phishing campaigns, malicious apps, or compromised websites. The malware can gain unauthorized access to devices. Once installed, it can perform extensive data exfiltration, including capturing keystrokes, recording audio, accessing files, and stealing credentials. The malware's ransomware capabilities can encrypt files on the infected device, demanding a ransom for their release. It also features Command and Control (C2) capabilities, allowing attackers to remotely manage infected devices and execute commands. 'com.velociraptor.raptor' is the package name of the malware sample. Constant strings in the code have been encrypted. The MD5 hash of this malware sample is 16c6c99d545d53957fbfe342f8f51903.</p>
Strike rafelrat_265c9114	<p>This strike sends a polymorphic malware sample known as Rafel RAT. Rafel RAT is a sophisticated Android malware that has evolved from espionage to ransomware operations. It is transmitted through phishing campaigns, malicious apps, or compromised websites. The malware can gain unauthorized access to devices. Once installed, it can perform extensive data exfiltration, including capturing keystrokes, recording audio, accessing files, and stealing credentials. The malware's ransomware capabilities can encrypt files on the infected device, demanding a ransom for their release. It also features Command and Control (C2) capabilities, allowing attackers to remotely manage infected devices and execute commands. 'com.velociraptor.raptor' is the package name of the malware sample. Constant strings in the code have been encrypted. The MD5 hash of this malware sample is 265c9114317096ce3dc73ebd2bd42720.</p>
Strike rafelrat_4a40410e	<p>This strike sends a malware sample known as Rafel RAT. Rafel RAT is a sophisticated Android malware that has evolved from espionage to ransomware operations. It is transmitted through phishing campaigns, malicious apps, or compromised websites. The malware can gain unauthorized access to devices. Once installed, it can perform extensive data exfiltration, including capturing keystrokes, recording audio, accessing files, and stealing credentials. The malware's ransomware capabilities can encrypt files on the infected device, demanding a ransom for their release. It also features Command and Control (C2) capabilities, allowing attackers to remotely manage infected devices and execute commands. 'com.velociraptor.raptor' is the package name of the malware sample. The MD5 hash of this malware sample is 4a40410e3ed082aa20d4eaa508ed451d.</p>
Strike rafelrat_76c68ac2	<p>This strike sends a polymorphic malware sample known as Rafel RAT. Rafel RAT is a sophisticated Android malware that has evolved from espionage to ransomware operations. It is transmitted through phishing campaigns, malicious apps, or compromised websites. The malware can gain unauthorized access to devices. Once installed, it can perform extensive data exfiltration, including capturing keystrokes, recording audio, accessing files, and stealing credentials. The malware's ransomware capabilities can encrypt files on the infected device, demanding a ransom for their release. It also features Command and Control (C2) capabilities, allowing attackers to remotely manage infected devices and execute commands. 'com.velociraptor.raptor' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 76c68ac2b02b6f960a63038c924720d0.</p>

<b>Name</b>	<b>Description</b>
Strike rafelrat_81791e8e	<p>This strike sends a polymorphic malware sample known as Rafel RAT. Rafel RAT is a sophisticated Android malware that has evolved from espionage to ransomware operations. It is transmitted through phishing campaigns, malicious apps, or compromised websites. The malware can gain unauthorized access to devices. Once installed, it can perform extensive data exfiltration, including capturing keystrokes, recording audio, accessing files, and stealing credentials. The malware's ransomware capabilities can encrypt files on the infected device, demanding a ransom for their release. It also features Command and Control (C2) capabilities, allowing attackers to remotely manage infected devices and execute commands. 'com.velociraptor.raptor' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 81791e8e349941fe83515ac5246e3e3d.</p>
Strike rafelrat_8abd7e06	<p>This strike sends a polymorphic malware sample known as Rafel RAT. Rafel RAT is a sophisticated Android malware that has evolved from espionage to ransomware operations. It is transmitted through phishing campaigns, malicious apps, or compromised websites. The malware can gain unauthorized access to devices. Once installed, it can perform extensive data exfiltration, including capturing keystrokes, recording audio, accessing files, and stealing credentials. The malware's ransomware capabilities can encrypt files on the infected device, demanding a ransom for their release. It also features Command and Control (C2) capabilities, allowing attackers to remotely manage infected devices and execute commands. 'com.velociraptor.raptor' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 8abd7e064c2cac2f39ce96414e5ae679.</p>
Strike rafelrat_94bca392	<p>This strike sends a malware sample known as Rafel RAT. Rafel RAT is a sophisticated Android malware that has evolved from espionage to ransomware operations. It is transmitted through phishing campaigns, malicious apps, or compromised websites. The malware can gain unauthorized access to devices. Once installed, it can perform extensive data exfiltration, including capturing keystrokes, recording audio, accessing files, and stealing credentials. The malware's ransomware capabilities can encrypt files on the infected device, demanding a ransom for their release. It also features Command and Control (C2) capabilities, allowing attackers to remotely manage infected devices and execute commands. 'com.velociraptor.raptor' is the package name of the malware sample. The MD5 hash of this malware sample is 94bca3926cd70f60d54be7218dd7ac55.</p>
Strike rafelrat_97af32bc	<p>This strike sends a polymorphic malware sample known as Rafel RAT. Rafel RAT is a sophisticated Android malware that has evolved from espionage to ransomware operations. It is transmitted through phishing campaigns, malicious apps, or compromised websites. The malware can gain unauthorized access to devices. Once installed, it can perform extensive data exfiltration, including capturing keystrokes, recording audio, accessing files, and stealing credentials. The malware's ransomware capabilities can encrypt files on the infected device, demanding a ransom for their release. It also features Command and Control (C2) capabilities, allowing attackers to remotely manage infected devices and execute commands. 'com.velociraptor.raptor' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 97af32bcdbe5f21ae6cf12d6164c31.</p>

<b>Name</b>	<b>Description</b>
Strike rafelrat_d92eecc4	<p>This strike sends a malware sample known as Rafel RAT. Rafel RAT is a sophisticated Android malware that has evolved from espionage to ransomware operations. It is transmitted through phishing campaigns, malicious apps, or compromised websites. The malware can gain unauthorized access to devices. Once installed, it can perform extensive data exfiltration, including capturing keystrokes, recording audio, accessing files, and stealing credentials. The malware's ransomware capabilities can encrypt files on the infected device, demanding a ransom for their release. It also features Command and Control (C2) capabilities, allowing attackers to remotely manage infected devices and execute commands 'com.velociraptor.raptor' is the package name of the malware sample. The MD5 hash of this malware sample is d92eecc462e59f3e2061a6a568935b96.</p>
Strike rafelrat_db1f53f	<p>This strike sends a polymorphic malware sample known as Rafel RAT. Rafel RAT is a sophisticated Android malware that has evolved from espionage to ransomware operations. It is transmitted through phishing campaigns, malicious apps, or compromised websites. The malware can gain unauthorized access to devices. Once installed, it can perform extensive data exfiltration, including capturing keystrokes, recording audio, accessing files, and stealing credentials. The malware's ransomware capabilities can encrypt files on the infected device, demanding a ransom for their release. It also features Command and Control (C2) capabilities, allowing attackers to remotely manage infected devices and execute commands 'com.velociraptor.raptor' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is dba1f53f3a50695c19dec79d24db94d3.</p>
Strike rafelrat_f630f576	<p>This strike sends a polymorphic malware sample known as Rafel RAT. Rafel RAT is a sophisticated Android malware that has evolved from espionage to ransomware operations. It is transmitted through phishing campaigns, malicious apps, or compromised websites. The malware can gain unauthorized access to devices. Once installed, it can perform extensive data exfiltration, including capturing keystrokes, recording audio, accessing files, and stealing credentials. The malware's ransomware capabilities can encrypt files on the infected device, demanding a ransom for their release. It also features Command and Control (C2) capabilities, allowing attackers to remotely manage infected devices and execute commands 'com.velociraptor.raptor' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is f630f576ea0f34c9d84de15af7d9196e.</p>
Strike rtospyware_41450833	<p>This strike sends a malware sample known as RTO spyware. The phishing campaign targets Android users in India and is designed to deceive individuals into providing personal and financial information through fake messages and websites mimicking the Regional Transport Office (RTO). The malware is distributed via WhatsApp, prompting users to click on malicious links. It collects device and contact data, sends this information to a Telegram bot, and uses Firebase to obtain phone numbers and text messages, facilitating unauthorized SMS verification. The campaign uses a Command and Control (C2) server and operates as a Malware-as-a-Service (MaaS). 'com.lijyutuportal.android' is the package name of the malware sample. The MD5 hash of this malware sample is 41450833c1eb6512843b2beb27e121c1.</p>

<b>Name</b>	<b>Description</b>
Strike rtospyware_84d4a9ae	This strike sends a polymorphic malware sample known as RTO spyware. The phishing campaign targets Android users in India and is designed to deceive individuals into providing personal and financial information through fake messages and websites mimicking the Regional Transport Office (RTO). The malware is distributed via WhatsApp, prompting users to click on malicious links. It collects device and contact data, sends this information to a Telegram bot, and uses Firebase to obtain phone numbers and text messages, facilitating unauthorized SMS verification. The campaign uses a Command and Control (C2) server and operates as a Malware-as-a-Service (MaaS). 'com.lijyutuportal.android' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 84d4a9ae06367527f078e11823ee25cf.
Strike rtospyware_a81082db	This strike sends a polymorphic malware sample known as RTO spyware. The phishing campaign targets Android users in India and is designed to deceive individuals into providing personal and financial information through fake messages and websites mimicking the Regional Transport Office (RTO). The malware is distributed via WhatsApp, prompting users to click on malicious links. It collects device and contact data, sends this information to a Telegram bot, and uses Firebase to obtain phone numbers and text messages, facilitating unauthorized SMS verification. The campaign uses a Command and Control (C2) server and operates as a Malware-as-a-Service (MaaS). 'com.lijyutuportal.android' is the package name of the malware sample. Constant strings in the code has been encrypted. The MD5 hash of this malware sample is a81082dbc6bb755766b35a13c13d75ce.
Strike rtospyware_f98858b8	This strike sends a polymorphic malware sample known as RTO spyware. The phishing campaign targets Android users in India and is designed to deceive individuals into providing personal and financial information through fake messages and websites mimicking the Regional Transport Office (RTO). The malware is distributed via WhatsApp, prompting users to click on malicious links. It collects device and contact data, sends this information to a Telegram bot, and uses Firebase to obtain phone numbers and text messages, facilitating unauthorized SMS verification. The campaign uses a Command and Control (C2) server and operates as a Malware-as-a-Service (MaaS). 'com.lijyutuportal.android' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is f98858b832960add10e27a546501615f.
Strike smseye_321fb949	This strike sends a malware sample known as smseye. It's an android malware which is designed to exfiltrate incoming SMS messages from infected Android devices, which are then sent to a designated Telegram chat controlled by the threat actors. This allows them to capture One-Time Passwords (OTPs) and bypass Multi-Factor Authentication (MFA) on the targeted accounts. The malware also requests permissions to send and view SMS messages under the guise of a security application for the victim's bank account. 'com.junior.course' is the package name of the malware sample. The MD5 hash of this smseye sample is acd79c2c79e1bac5b3b564bb7a62bcd8. The manifest file of the malware has been randomly rearranged.

Name	Description
Strike smseye_3a48fd36	This strike sends a malware sample known as smseye. It's an android malware which is designed to exfiltrate incoming SMS messages from infected Android devices, which are then sent to a designated Telegram chat controlled by the threat actors. This allows them to capture One-Time Passwords (OTPs) and bypass Multi-Factor Authentication (MFA) on the targeted accounts. The malware also requests permissions to send and view SMS messages under the guise of a security application for the victim's bank account. 'com.junior.course' is the package name of the malware sample. The MD5 hash of this smseye sample is acd79c2c79e1bac5b3b564bb7a62bcd8. The malware has been rebuilt without any modifications.
Strike smseye_acd79c2c	This strike sends a malware sample known as smseye. It's an android malware which is designed to exfiltrate incoming SMS messages from infected Android devices, which are then sent to a designated Telegram chat controlled by the threat actors. This allows them to capture One-Time Passwords (OTPs) and bypass Multi-Factor Authentication (MFA) on the targeted accounts. The malware also requests permissions to send and view SMS messages under the guise of a security application for the victim's bank account. 'com.junior.course' is the package name of the malware sample. The MD5 hash of this smseye sample is acd79c2c79e1bac5b3b564bb7a62bcd8.
Strike soco404_14bf32e7	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is 14bf32e780601c6870811982648cf293.
Strike soco404_229df8da	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is 229df8dab03385371464e9a5f3ee89bd.
Strike soco404_2a26af6c	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is 2a26af6c46ffb18509397b2ec7f9389a.
Strike soco404_35b66458	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is 35b6645859a2fc674042e284879be11.

<b>Name</b>	<b>Description</b>
Strike soco404_6a267dfa	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is 6a267dfa08378eab14650b8d5fda6171.
Strike soco404_71309198	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is 713091980135a30a452b34026d949890.
Strike soco404_7feedc2c	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is 7feedc2cd91f037d1bcd9285e6f1341b.
Strike soco404_ac00592c	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is ac00592cb93fbb64c26b7f99cfcb80be.
Strike soco404_bb8fbe0f	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is bb8fbe0f257508c78df00252de2fa48c.
Strike soco404_bd8ce6bd	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is bd8ce6bd59b1f648e0ac38e575780453.
Strike soco404_c95ab34d	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is c95ab34d79740f5fa5fdc211c35eb5ea.
Strike soco404_ca125aba	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is ca125aba3e130e2d6a122fcc76461fdc.

<b>Name</b>	<b>Description</b>
Strike soco404_d2226fa9	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is d2226fa9e050f8fd5fe3d4aae27d3406.
Strike soco404_fa904f9d	This strike sends a malware sample known as soco404. soco404 targets Linux and Windows systems with misconfigured PostgreSQL, Apache Tomcat, and other exposed services. It hides payloads within benign seeming fake 404 HTML pages. It uses in memory execution and process masquerading, and aims to mine Monero profitably while avoiding detection. The MD5 hash of this soco404 sample is fa904f9d5abecd5e62645b115f30d971.
Strike spyloan_33758feb	This strike sends a polymorphic malware sample known as SpyLoan. SpyLoan masquerades as a legitimate financial loan app, distributed through social engineering tactics. The malware targets users by exploiting their trust and urgency, often through fake loan offers. The malware collects extensive personal information, including contact lists, SMS data, and call logs, which are then used to harass and extort victims. It also communicates with command-and-control (C2) servers to exfiltrate stolen data. 'com.prestamoseguro.ss' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 33758feba989a613a43d0dcefc605d41.
Strike spyloan_402ea7dd	This strike sends a polymorphic malware sample known as SpyLoan. SpyLoan masquerades as a legitimate financial loan app, distributed through social engineering tactics. The malware targets users by exploiting their trust and urgency, often through fake loan offers. The malware collects extensive personal information, including contact lists, SMS data, and call logs, which are then used to harass and extort victims. It also communicates with command-and-control (C2) servers to exfiltrate stolen data. 'com.gotoloan.cash' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 402ea7dd87ce9f16aeff53a60384b98e.
Strike spyloan_65569678	This strike sends a polymorphic malware sample known as SpyLoan. SpyLoan masquerades as a legitimate financial loan app, distributed through social engineering tactics. The malware targets users by exploiting their trust and urgency, often through fake loan offers. The malware collects extensive personal information, including contact lists, SMS data, and call logs, which are then used to harass and extort victims. It also communicates with command-and-control (C2) servers to exfiltrate stolen data. 'com.prestamoseguro.ss' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 655696788c65ae3d63cdbfc4d963d352.
Strike spyloan_6d754955	This strike sends a malware sample known as SpyLoan. SpyLoan masquerades as a legitimate financial loan app, distributed through social engineering tactics. The malware targets users by exploiting their trust and urgency, often through fake loan offers. The malware collects extensive personal information, including contact lists, SMS data, and call logs, which are then used to harass and extort victims. It also communicates with command-and-control (C2) servers to exfiltrate stolen data. 'com.prestamoseguro.ss' is the package name of the malware sample. The MD5 hash of this malware sample is 6d754955a0106fc17b0996f669324ac0.

<b>Name</b>	<b>Description</b>
Strike spyloan_b5fb3677	<p>This strike sends a polymorphic malware sample known as SpyLoan. SpyLoan masquerades as a legitimate financial loan app, distributed through social engineering tactics. The malware targets users by exploiting their trust and urgency, often through fake loan offers. The malware collects extensive personal information, including contact lists, SMS data, and call logs, which are then used to harass and extort victims. It also communicates with command-and-control (C2) servers to exfiltrate stolen data. 'com.gotoloan.cash' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is b5fb3677c7f54cac2b2114b354ba04f7.</p>
Strike spyloan_bca86a7a	<p>This strike sends a malware sample known as SpyLoan. SpyLoan masquerades as a legitimate financial loan app, distributed through social engineering tactics. The malware targets users by exploiting their trust and urgency, often through fake loan offers. The malware collects extensive personal information, including contact lists, SMS data, and call logs, which are then used to harass and extort victims. It also communicates with command-and-control (C2) servers to exfiltrate stolen data. 'com.gotoloan.cash' is the package name of the malware sample. The MD5 hash of this malware sample is bca86a7ac6874056f9ce114367038e0e.</p>
Strike spyloan_e4b1c610	<p>This strike sends a polymorphic malware sample known as SpyLoan. SpyLoan masquerades as a legitimate financial loan app, distributed through social engineering tactics. The malware targets users by exploiting their trust and urgency, often through fake loan offers. The malware collects extensive personal information, including contact lists, SMS data, and call logs, which are then used to harass and extort victims. It also communicates with command-and-control (C2) servers to exfiltrate stolen data. 'com.voscp.rapido' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is e4b1c610ee59c67dfc05555752c347fd.</p>
Strike spyloan_e4da2096	<p>This strike sends a malware sample known as SpyLoan. SpyLoan masquerades as a legitimate financial loan app, distributed through social engineering tactics. The malware targets users by exploiting their trust and urgency, often through fake loan offers. The malware collects extensive personal information, including contact lists, SMS data, and call logs, which are then used to harass and extort victims. It also communicates with command-and-control (C2) servers to exfiltrate stolen data. 'com.voscp.rapido' is the package name of the malware sample. The MD5 hash of this malware sample is e4da2096c972441afa1ffd5f264b4b35.</p>
Strike spyloan_e9c19f84	<p>This strike sends a polymorphic malware sample known as SpyLoan. SpyLoan masquerades as a legitimate financial loan app, distributed through social engineering tactics. The malware targets users by exploiting their trust and urgency, often through fake loan offers. The malware collects extensive personal information, including contact lists, SMS data, and call logs, which are then used to harass and extort victims. It also communicates with command-and-control (C2) servers to exfiltrate stolen data. 'com.voscp.rapido' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is e9c19f84e5256ddbad1c47394d6a649f.</p>

<b>Name</b>	<b>Description</b>
Strike spyloan_ec382de4	This strike sends a polymorphic malware sample known as SpyLoan. SpyLoan masquerades as a legitimate financial loan app, distributed through social engineering tactics. The malware targets users by exploiting their trust and urgency, often through fake loan offers. The malware collects extensive personal information, including contact lists, SMS data, and call logs, which are then used to harass and extort victims. It also communicates with command-and-control (C2) servers to exfiltrate stolen data. 'com.gotoloan.cash' is the package name of the malware sample. Constant strings in the code has been encrypted. The MD5 hash of this malware sample is ec382de4f05e45b14d94b4f1a130295b.
Strike spynote_026fae1c	This strike sends a polymorphic malware sample known as SpyNote. SpyNote is a sophisticated Remote Access Trojan (RAT) that has evolved to target cryptocurrency wallets on Android devices. It exploits the Accessibility API to automatically perform malicious actions such as recording unlocking gestures and transferring cryptocurrency without user intervention. Disguised as legitimate applications, including crypto wallets, SpyNote tricks users into granting necessary permissions, then overlays fake screens on top of real apps to redirect cryptocurrency transactions to the attackers' wallets stealthily. 'com.miui.tencent.security' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 026fae1c816399a5c18da7b70567b70e.
Strike spynote_3f59e1ea	This strike sends a malware sample known as SpyNote. SpyNote is a sophisticated Remote Access Trojan (RAT) that has evolved to target cryptocurrency wallets on Android devices. It exploits the Accessibility API to automatically perform malicious actions such as recording unlocking gestures and transferring cryptocurrency without user intervention. Disguised as legitimate applications, including crypto wallets, SpyNote tricks users into granting necessary permissions, then overlays fake screens on top of real apps to redirect cryptocurrency transactions to the attackers' wallets stealthily. 'com.miui.tencent.security' is the package name of the malware sample. The MD5 hash of this malware sample is 3f59e1ea2c222a211f5643e50a256875.
Strike spynote_92df3770	This strike sends a malware sample known as SpyNote. SpyNote is a sophisticated Remote Access Trojan (RAT) that has evolved to target cryptocurrency wallets on Android devices. It exploits the Accessibility API to automatically perform malicious actions such as recording unlocking gestures and transferring cryptocurrency without user intervention. Disguised as legitimate applications, including crypto wallets, SpyNote tricks users into granting necessary permissions, then overlays fake screens on top of real apps to redirect cryptocurrency transactions to the attackers' wallets stealthily. 'com.miui.tencent.security' is the package name of the malware sample. The MD5 hash of this malware sample is 92df3770e6426013880eb177389f27f3.

<b>Name</b>	<b>Description</b>
Strike spynote_aa2e9c25	<p>This strike sends a polymorphic malware sample known as SpyNote. SpyNote is a sophisticated Remote Access Trojan (RAT) that has evolved to target cryptocurrency wallets on Android devices. It exploits the Accessibility API to automatically perform malicious actions such as recording unlocking gestures and transferring cryptocurrency without user intervention. Disguised as legitimate applications, including crypto wallets, SpyNote tricks users into granting necessary permissions, then overlays fake screens on top of real apps to redirect cryptocurrency transactions to the attackers' wallets stealthily. 'com.miui.tencent.security' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is aa2e9c25f24cccd6bde45040ab78831cb.</p>
Strike spynote_b924910c	<p>This strike sends a polymorphic malware sample known as SpyNote. SpyNote is a sophisticated Remote Access Trojan (RAT) that has evolved to target cryptocurrency wallets on Android devices. It exploits the Accessibility API to automatically perform malicious actions such as recording unlocking gestures and transferring cryptocurrency without user intervention. Disguised as legitimate applications, including crypto wallets, SpyNote tricks users into granting necessary permissions, then overlays fake screens on top of real apps to redirect cryptocurrency transactions to the attackers' wallets stealthily. 'com.miui.tencent.security' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is b924910c659e2c60085c803d510424bd.</p>
Strike spynote_db759a4d	<p>This strike sends a polymorphic malware sample known as SpyNote. SpyNote is a sophisticated Remote Access Trojan (RAT) that has evolved to target cryptocurrency wallets on Android devices. It exploits the Accessibility API to automatically perform malicious actions such as recording unlocking gestures and transferring cryptocurrency without user intervention. Disguised as legitimate applications, including crypto wallets, SpyNote tricks users into granting necessary permissions, then overlays fake screens on top of real apps to redirect cryptocurrency transactions to the attackers' wallets stealthily. 'com.miui.tencent.security' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is db759a4d12b35ce2083c4c2ad7b09194.</p>
Strike triada_2ac4d8e1	<p>This strike sends a malware sample known as triada. triada is android malware which has now been detected posing as many popular apps including, Telegram, WhatsApp, Instagram, TikTok, Facebook, Skype, and Google Play. The malware signs the user up for paid subscriptions, performs in-app purchases using the user's SMS and phone number, displays advertisements, and steals login credentials and other user and device information. Depending on the specific app module, the malware behave differently in how it connects outbound to the C2 server. This sample was detected within native libraries included in the firmware of mobile Android devices. The MD5 hash of this triada sample is 2ac4d8e1077dce6f4d2ba9875b987ca7.</p>

<b>Name</b>	<b>Description</b>
Strike triada_716f0896	This strike sends a malware sample known as triada. triada is android malware which has now been detected posing as many popular apps including, Telegram, WhatsApp, Instagram, TikTok, Facebook, Skype, and Google Play. The malware signs the user up for paid subscriptions, performs in-app purchases using the user's SMS and phone number, displays advertisements, and steals login credentials and other user and device information. Depending on the specific app module, the malware behave differently in how it connects outbound to the C2 server. This sample was detected within native libraries included in the firmware of mobile Android devices. The MD5 hash of this triada sample is 716f0896b22c2fdcb0e3ee56b7c5212f.
Strike triada_89c3475b	This strike sends a malware sample known as triada. triada is android malware which has now been detected posing as many popular apps including, Telegram, WhatsApp, Instagram, TikTok, Facebook, Skype, and Google Play. The malware signs the user up for paid subscriptions, performs in-app purchases using the user's SMS and phone number, displays advertisements, and steals login credentials and other user and device information. Depending on the specific app module, the malware behave differently in how it connects outbound to the C2 server. This sample was detected within native libraries included in the firmware of mobile Android devices. The MD5 hash of this triada sample is 89c3475be8dba92f4ee7de0d981603c1.
Strike triada_c30c309e	This strike sends a malware sample known as triada. triada is android malware which has now been detected posing as many popular apps including, Telegram, WhatsApp, Instagram, TikTok, Facebook, Skype, and Google Play. The malware signs the user up for paid subscriptions, performs in-app purchases using the user's SMS and phone number, displays advertisements, and steals login credentials and other user and device information. Depending on the specific app module, the malware behave differently in how it connects outbound to the C2 server. This sample was detected within native libraries included in the firmware of mobile Android devices. The MD5 hash of this triada sample is c30c309e175905ffcbd17adb55009240.
Strike triada_fb937b1b	This strike sends a malware sample known as triada. triada is android malware which has now been detected posing as many popular apps including, Telegram, WhatsApp, Instagram, TikTok, Facebook, Skype, and Google Play. The malware signs the user up for paid subscriptions, performs in-app purchases using the user's SMS and phone number, displays advertisements, and steals login credentials and other user and device information. Depending on the specific app module, the malware behave differently in how it connects outbound to the C2 server. This sample was detected within native libraries included in the firmware of mobile Android devices. The MD5 hash of this triada sample is fb937b1b15fd56c9d8e5bb6b90e0e24a.

Name	Description
Strike vahan_0837b316	This strike sends a polymorphic malware sample known as SpyMax. The malware masquerades as an application from the humanitarian organization CARE International to deceive users. The application requests excessive and invasive permissions, including access to the phone's camera, audio, SMS, contacts, internet, WiFi, and external storage (read and write permissions). Such extensive permission requests are indicative of the malware's intent to compromise user privacy and security, potentially allowing it to monitor and control various aspects of the device without the user's consent. 'com.orgnimilicareat.il0' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 0837b316ab674596618dae9d7357f312.
Strike vahan_33b61328	This strike sends a polymorphic malware sample known as VAHAN PARIVAHAN. The phishing campaign targets Android users in India and is designed to deceive individuals into providing personal and financial information through fake messages and websites mimicking the Regional Transport Office (RTO). The malware is distributed via WhatsApp, prompting users to click on malicious links. It collects device and contact data, sends this information to a Telegram bot, and uses Firebase to obtain phone numbers and text messages, facilitating unauthorized SMS verification. The campaign uses a Command and Control (C2) server and operates as a Malware-as-a-Service (MaaS). 'eruyy.yrry' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 33b613285e305a6a8ae5fea7a495ec82.
Strike vahan_468de34b	This strike sends a malware sample known as SpyMax. The malware masquerades as an application from the humanitarian organization CARE International to deceive users. The application requests excessive and invasive permissions, including access to the phone's camera, audio, SMS, contacts, internet, WiFi, and external storage (read and write permissions). Such extensive permission requests are indicative of the malware's intent to compromise user privacy and security, potentially allowing it to monitor and control various aspects of the device without the user's consent. 'com.orgnimilicareat.il0' is the package name of the malware sample. The MD5 hash of this malware sample is 468de34b866e9542f1fe58d51d7c9d8a.
Strike vahan_6bd07f66	This strike sends a polymorphic malware sample known as VAHAN PARIVAHAN. The phishing campaign targets Android users in India and is designed to deceive individuals into providing personal and financial information through fake messages and websites mimicking the Regional Transport Office (RTO). The malware is distributed via WhatsApp, prompting users to click on malicious links. It collects device and contact data, sends this information to a Telegram bot, and uses Firebase to obtain phone numbers and text messages, facilitating unauthorized SMS verification. The campaign uses a Command and Control (C2) server and operates as a Malware-as-a-Service (MaaS). 'eruyy.yrry' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is 6bd07f66da0373b93f783d03da10ae28.

Name	Description
Strike vahan_91f2ba7f	This strike sends a malware sample known as VAHAN PARIVAHAN. The phishing campaign targets Android users in India and is designed to deceive individuals into providing personal and financial information through fake messages and websites mimicking the Regional Transport Office (RTO). The malware is distributed via WhatsApp, prompting users to click on malicious links. It collects device and contact data, sends this information to a Telegram bot, and uses Firebase to obtain phone numbers and text messages, facilitating unauthorized SMS verification. The campaign uses a Command and Control (C2) server and operates as a Malware-as-a-Service (MaaS). 'eruyy.yrry' is the package name of the malware sample. The MD5 hash of this malware sample is 961ede4f131f3a7322863ef99cc446b5.
Strike vahan_a12dbc76	This strike sends a polymorphic malware sample known as SpyMax. The malware masquerades as an application from the humanitarian organization CARE International to deceive users. The application requests excessive and invasive permissions, including access to the phone's camera, audio, SMS, contacts, internet, WiFi, and external storage (read and write permissions). Such extensive permission requests are indicative of the malware's intent to compromise user privacy and security, potentially allowing it to monitor and control various aspects of the device without the user's consent. 'com.orgnimilicareat.ilo' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is a12dbc768d38185a1397cf3d85eb5015.
Strike vahan_a7ec53e8	This strike sends a polymorphic malware sample known as VAHAN PARIVAHAN. The phishing campaign targets Android users in India and is designed to deceive individuals into providing personal and financial information through fake messages and websites mimicking the Regional Transport Office (RTO). The malware is distributed via WhatsApp, prompting users to click on malicious links. It collects device and contact data, sends this information to a Telegram bot, and uses Firebase to obtain phone numbers and text messages, facilitating unauthorized SMS verification. The campaign uses a Command and Control (C2) server and operates as a Malware-as-a-Service (MaaS). 'eruyy.yrry' is the package name of the malware sample. Constant strings in the code have been encrypted. The MD5 hash of this malware sample is a7ec53e808ca3b939ebd855d2e4bd4f4.
Strike vahan_c4cb8314	This strike sends a polymorphic malware sample known as SpyMax. The malware masquerades as an application from the humanitarian organization CARE International to deceive users. The application requests excessive and invasive permissions, including access to the phone's camera, audio, SMS, contacts, internet, WiFi, and external storage (read and write permissions). Such extensive permission requests are indicative of the malware's intent to compromise user privacy and security, potentially allowing it to monitor and control various aspects of the device without the user's consent. 'com.orgnimilicareat.ilo' is the package name of the malware sample. Constant strings in the code have been encrypted. The MD5 hash of this malware sample is c4cb83147f65c31198c5e26e89e6214f.

<b>Name</b>	<b>Description</b>
Strike wroba_abe91fc8	<p>This strike sends a polymorphic malware sample known as Wroba.o/XLoader. It is an android malware that has been recently updated to include a DNS changer module. This allows the malware to hijack routers and redirect devices that connect to the router to malicious websites. The malware is typically distributed through phishing campaigns, where users are tricked into clicking on a link or downloading an attachment that contains the malware. Once installed on a device, Wroba.o/XLoader can steal personal data, install other malware, and even take control of the device. The addition of a DNS changer module makes Wroba.o/XLoader even more dangerous, as it can now spread to other devices on the same network. This means that if one device on a network is infected with this malware then, all other devices on the network are also at risk. 'yy.wtkvds.lhmrgg.cim' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is abe91fc864fd6b7975cd2ed365923a3c.</p>
Strike wroba_dfac5971	<p>This strike sends a polymorphic malware sample known as Wroba.o/XLoader. It is an android malware that has been recently updated to include a DNS changer module. This allows the malware to hijack routers and redirect devices that connect to the router to malicious websites. The malware is typically distributed through phishing campaigns, where users are tricked into clicking on a link or downloading an attachment that contains the malware. Once installed on a device, Wroba.o/XLoader can steal personal data, install other malware, and even take control of the device. The addition of a DNS changer module makes Wroba.o/XLoader even more dangerous, as it can now spread to other devices on the same network. This means that if one device on a network is infected with this malware then, all other devices on the network are also at risk. 'yy.wtkvds.lhmrgg.cim' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is dfac597173ad4480954a40d5c840b8ac.</p>
Strike wroba_f9e43cc7	<p>This strike sends a malware sample known as Wroba.o/XLoader. It is an android malware that has been recently updated to include a DNS changer module. This allows the malware to hijack routers and redirect devices that connect to the router to malicious websites. The malware is typically distributed through phishing campaigns, where users are tricked into clicking on a link or downloading an attachment that contains the malware. Once installed on a device, Wroba.o/XLoader can steal personal data, install other malware, and even take control of the device. The addition of a DNS changer module makes Wroba.o/XLoader even more dangerous, as it can now spread to other devices on the same network. This means that if one device on a network is infected with this malware then, all other devices on the network are also at risk. 'yy.wtkvds.lhmrgg.cim' is the package name of the malware sample. The MD5 hash of this malware sample is f9e43cc73f040438243183e1faf46581.</p>
Strike wyrmspy_16be804c	<p>This strike sends a polymorphic malware sample known as wyrmspy. It's an android malware which uses rooting tools to elevate its privileges on the device. It then carries out surveillance tasks based on instructions it receives from its command and control (C2) servers. These instructions encompass actions such as directing the malware to transfer log files, retrieve photos from the device, and gather device location information through the utilization of the Baidu Location library. The malware infiltrates systems under the guise of innocuous-looking applications. 'com.sec.android.provider.badge' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this wyrmspy sample is 16be804c03588a54930cb1a1902319b2.</p>

<b>Name</b>	<b>Description</b>
Strike wyrmspy_21439e20	<p>This strike sends a polymorphic malware sample known as wyrmspy. It's an android malware which uses rooting tools to elevate its privileges on the device. It then carries out surveillance tasks based on instructions it receives from its command and control (C2) servers. These instructions encompass actions such as directing the malware to transfer log files, retrieve photos from the device, and gather device location information through the utilization of the Baidu Location library. The malware infiltrates systems under the guise of innocuous-looking applications.</p> <p>'com.sec.android.provider.badge' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this wyrmspy sample is 21439e2066c558510f6219c8ac7255d5.</p>
Strike wyrmspy_66342e3d	<p>This strike sends a polymorphic malware sample known as wyrmspy. It's an android malware which uses rooting tools to elevate its privileges on the device. It then carries out surveillance tasks based on instructions it receives from its command and control (C2) servers. These instructions encompass actions such as directing the malware to transfer log files, retrieve photos from the device, and gather device location information through the utilization of the Baidu Location library. The malware infiltrates systems under the guise of innocuous-looking applications.</p> <p>'com.sec.android.provider.badge' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this wyrmspy sample is 66342e3d0e2a066aa66c00e8103b9027.</p>
Strike wyrmspy_fe7ab00c	<p>This strike sends a polymorphic malware sample known as wyrmspy. It's an android malware which uses rooting tools to elevate its privileges on the device. It then carries out surveillance tasks based on instructions it receives from its command and control (C2) servers. These instructions encompass actions such as directing the malware to transfer log files, retrieve photos from the device, and gather device location information through the utilization of the Baidu Location library. The malware infiltrates systems under the guise of innocuous-looking applications.</p> <p>'com.sec.android.provider.badge' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this wyrmspy sample is fe7ab00c4d7f0c2b343e61473ff24cee.</p>
Strike xCry_7475713d	<p>This strike sends a malware sample known as xCry. xCry is a ransomware that is written in Nim and can easily be adapted to work across multiple platforms. The MD5 hash of this xCry sample is 7475713df82b2a81b2d32715a94c2b63.</p>
Strike zanubis_054061a4	<p>This strike sends a malware sample known as Zanubis. Zanubis is an Android banking Trojan that disguises itself as trusted apps, like the Peruvian government's SUNAT app, to target financial and cryptocurrency users in Peru. It gains control by tricking users into granting Accessibility permissions and uses obfuscation techniques for evasion. Once inside a device, it appears legitimate by loading genuine websites. Zanubis maintains connectivity to a controlling server and can adapt to steal data from specific apps while potentially gaining full control of the device. It can also disable a device by posing as an Android system update, rendering it unusable. 'at.au.av' is the package name of the malware sample. The MD5 hash of this malware sample is 054061a4f0c37b0b353580f644eac554.</p>

<b>Name</b>	<b>Description</b>
Strike zanubis_248b2b76	This strike sends a malware sample known as Zanubis. Zanubis is an Android banking Trojan that disguises itself as trusted apps, like the Peruvian government's SUNAT app, to target financial and cryptocurrency users in Peru. It gains control by tricking users into granting Accessibility permissions and uses obfuscation techniques for evasion. Once inside a device, it appears legitimate by loading genuine websites. Zanubis maintains connectivity to a controlling server and can adapt to steal data from specific apps while potentially gaining full control of the device. It can also disable a device by posing as an Android system update, rendering it unusable. 'at.au.av' is the package name of the malware sample. The MD5 hash of this malware sample is 248b2b76b5fb6e35c2d0a8657e080759.
Strike zanubis_5f1f70d4	This strike sends a polymorphic malware sample known as Zanubis. Zanubis is an Android banking Trojan that disguises itself as trusted apps, like the Peruvian government's SUNAT app, to target financial and cryptocurrency users in Peru. It gains control by tricking users into granting Accessibility permissions and uses obfuscation techniques for evasion. Once inside a device, it appears legitimate by loading genuine websites. Zanubis maintains connectivity to a controlling server and can adapt to steal data from specific apps while potentially gaining full control of the device. It can also disable a device by posing as an Android system update, rendering it unusable. 'at.au.av' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is 5f1f70d4f4baaf20448593e10c4971a.
Strike zanubis_a487e70a	This strike sends a polymorphic malware sample known as Zanubis. Zanubis is an Android banking Trojan that disguises itself as trusted apps, like the Peruvian government's SUNAT app, to target financial and cryptocurrency users in Peru. It gains control by tricking users into granting Accessibility permissions and uses obfuscation techniques for evasion. Once inside a device, it appears legitimate by loading genuine websites. Zanubis maintains connectivity to a controlling server and can adapt to steal data from specific apps while potentially gaining full control of the device. It can also disable a device by posing as an Android system update, rendering it unusable. 'at.au.av' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is a487e70a88776e37bee3fbf0caab1515.
Strike zanubis_d70e6ec1	This strike sends a polymorphic malware sample known as Zanubis. Zanubis is an Android banking Trojan that disguises itself as trusted apps, like the Peruvian government's SUNAT app, to target financial and cryptocurrency users in Peru. It gains control by tricking users into granting Accessibility permissions and uses obfuscation techniques for evasion. Once inside a device, it appears legitimate by loading genuine websites. Zanubis maintains connectivity to a controlling server and can adapt to steal data from specific apps while potentially gaining full control of the device. It can also disable a device by posing as an Android system update, rendering it unusable. 'at.au.av' is the package name of the malware sample. The malware has been rebuilt without any modifications. The MD5 hash of this malware sample is d70e6ec1f916949f8f1293ffd5c7e386.

<b>Name</b>	<b>Description</b>
Strike zanubis_e2954c6b	This strike sends a polymorphic malware sample known as Zanubis. Zanubis is an Android banking Trojan that disguises itself as trusted apps, like the Peruvian government's SUNAT app, to target financial and cryptocurrency users in Peru. It gains control by tricking users into granting Accessibility permissions and uses obfuscation techniques for evasion. Once inside a device, it appears legitimate by loading genuine websites. Zanubis maintains connectivity to a controlling server and can adapt to steal data from specific apps while potentially gaining full control of the device. It can also disable a device by posing as an Android system update, rendering it unusable. 'at.au.av' is the package name of the malware sample. The manifest file of the malware has been randomly rearranged. The MD5 hash of this malware sample is e2954c6bfc0d6dd17c346324e4926edb.
Strike zbot_0552f6d8	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is 0552f6d8a414b14d68fd1a6107cb61fa.
Strike zbot_092ba799	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is 092ba7998e57d75a810407713a98989d.
Strike zbot_0d08e1a5	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is 0d08e1a548cefdbc2b15319141495c7b.
Strike zbot_167e959c	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is 167e959ce5a8932eb077574c3f75cb0e.
Strike zbot_21a2c4ed	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is 21a2c4ede651ec95e613f7b3d5a92576.
Strike zbot_2f53bbc1	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this zbot sample is 2f53bbc18fbde76c9af44080c8a27d4f.
Strike zbot_2fd300e3	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is 2fd300e3141914d38f4667ed39ce42e7.
Strike zbot_3dac3605	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this zbot sample is 3dac3605c4ae1393ba10e210bdd0dbb4.

<b>Name</b>	<b>Description</b>
Strike zbot_3db93690	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is 3db9369025c1e1df47571f99b3ffde91.
Strike zbot_3e2cc76b	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this zbot sample is 3e2cc76b4f3130cac9a0c7226e8241bc.
Strike zbot_40e81faf	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this zbot sample is 40e81faf9b2e9988038bf366660f58e9.
Strike zbot_40eb666a	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is 40eb666a6b89be8f8059b2d7eb0e5c79.
Strike zbot_47a8a927	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has random strings (lorem ipsum) appended at the end of the file. The MD5 hash of this zbot sample is 47a8a927adaad09e5ac0de66e8645e81.
Strike zbot_48f608eb	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this zbot sample is 48f608ebadfe7397c27c79d8ce93d8.
Strike zbot_50a14e9b	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is 50a14e9b468fe0b6f4df1644f9bec11d.
Strike zbot_50ec927e	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has the checksum removed in the PE file format. The MD5 hash of this zbot sample is 50ec927e11de865805d6a1a773a7214b.
Strike zbot_60adbecd	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is 60adbecd077b22b9ef6d3c77234d8698.
Strike zbot_721fd397	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is 721fd397c03d99ba839229a3952eebf1.

<b>Name</b>	<b>Description</b>
Strike zbot_7d216a6f	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is 7d216a6f51c49156c643c82bb74b0c6b.
Strike zbot_7d57d787	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is 7d57d78703808c1a743c63da9c112560.
Strike zbot_88f44e93	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is 88f44e9374e90e6590826c43b86c8c9e.
Strike zbot_8a11c833	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has random bytes appended at the end of the file. The MD5 hash of this zbot sample is 8a11c8335b613621a0827b3067a9c873.
Strike zbot_aa0f603d	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is aa0f603defa713c48c53c1c45b040b00.
Strike zbot_abf36547	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is abf36547b0503378c8b7db8d35f2c2b9.
Strike zbot_adf85bd5	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has the checksum removed in the PE file format. The MD5 hash of this zbot sample is adf85bd56291f66ca26fb77708f7cd59.
Strike zbot_b1e05e32	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is b1e05e328459d12897603aa428a025e9.
Strike zbot_baadcc21	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is baadcc21e1cc730a6c04cfb7d2e06d4b.
Strike zbot_be866d7f	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has random contents appended in one of the existing sections in the PE file format. The MD5 hash of this zbot sample is be866d7f489ad00b66fddae7a3bdc47c.
Strike zbot_c1cc71f0	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has the checksum removed in the PE file format. The MD5 hash of this zbot sample is c1cc71f052333c76f1f2d8891948491f.

<b>Name</b>	<b>Description</b>
Strike zbot_ce11c0cd	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is ce11c0cd78c9ce812bd57bc0a18868e6.
Strike zbot_d666d3a1	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is d666d3a1431461045cf597c434f6e916.
Strike zbot_d84b5ff0	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has random bytes appended at the end of the file. The MD5 hash of this zbot sample is d84b5ff09729a9f794e3acc44fcc1bfc.
Strike zbot_e04090aa	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has random bytes appended at the end of the file. The MD5 hash of this zbot sample is e04090aafc9a3426053ed869abb27292.
Strike zbot_e2a2497b	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is e2a2497b7f4cd8dd96cf088316b8da70.
Strike zbot_ed5fa845	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this zbot sample is ed5fa845cdbd920d901d1739d8045836.
Strike zbot_f6fd7429	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is f6fd7429ff3fcc0ff4ee3757099a36ae.
Strike zbot_fb74cf88	This strike sends a malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The MD5 hash of this zbot sample is fb74cf88d476e3308527b9a18fa4adc8.
Strike zbot_fc57f83f	This strike sends a polymorphic malware sample known as zbot. Zbot also known as Zeus is a trojan often associated with stealing banking information by keystroke logging and form grabbing techniques. The binary has a random section name renamed according to the PE format specification. The MD5 hash of this zbot sample is fc57f83f679664e14da2f7cc2f257036.